

CEH Certified Ethical Hacker More Than 100 Success Secrets

Over 100 Professional
Security Testers Most
Asked Questions and
Resources

Ronald White

CEH Certified Ethical Hacker More Than 100 Success Secrets: Over 100 Professional Security Testers Most Asked Questions and Resources

CEH 100 Success Secrets

Copyright(c) 2008

Notice of rights

All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

Notice of Liability

The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

CEH 100 Success Secrets

There has never been a CEH Guide like this.

100 Success Secrets is *not* about the ins and outs of CEH. Instead, it answers the top 100 questions that we are asked and those we come across in forums, our consultancy and education programs.

It tells you exactly how to deal with those questions, with tips that have never before been offered in print.

This book is also *not* about CEH' best practice and standards details. Instead, it introduces everything you want to know to be successful with CEH.

Table of Contents

CEH Certified Ethical Hacker More Than 100 Success Secrets:1	
Over 100 Professional Security Testers Most Asked Questions and Resources	1
Key Elements of Physical Security	12
Proxy Server Technologies: The Lowdown	13
Multiple Ways of Scanning Your Computer Data	14
Session Hijacking: Need to Know Information on Protection	15
Social Engineering: Why You Should Be Wary	16
How to Get Certified an Anti Spamming Practitioner	17
How Hackers perform SQL Injection and How to Fight It?	19
Two Methods of Training for CEH Certification Exam	21
Understanding Viruses and Worms and the Ways to Disinfect Your Computer.....	23
Top Two Web Application Vulnerabilities	25
Privacy on the Internet: Why It Pays to Be Aware.....	27
The Alarming Abundance of RFID Hacking Actions.....	28
Two Great Ways of Securing Laptop Computers	29
A Word about Sniffers and Cyber Theft.....	30
The Current State of Software Piracy and Warez.....	31
Types of Computer Spying Technologies	32
How to Prevent System Hacking.....	34
How Trojans and Backdoors Work to Wreck Havoc on Your	

System	36
How to Minimize the Risk of VoIP Hacking.....	38
Common Types of Web-Based Password Cracking Techniques	40
The Ultimate Guide towards Hacking USB Devices	42
The Effective Techniques towards Better Internet Content Filtering.....	43
An Explosive Revelation about hacking a Linux System.....	45
The Advantages of an Online CEH Certification	46
Data Recovery: A Fundamental Online CEH Training	48
The Effective Online Program to deliver the best Certified Ethical Hacker	49
The Designed Online Courses for Certified Ethical Hackers	50
Effective Online Training for an On-site CEH	52
Can you hack a Site using your Web Browser like Firefox?	53
A Broad Introduction to Ethical Hacking	54
The Realities about Hacking a Macintosh System.....	55
Internet Security: A Favorite Online CEH Course	57
Become a Certified Ethical Hacker by taking the online Certification.....	59
Online Schools for Certified Ethical Hackers	61
Taking CEH On-site Certification.....	62
Understanding the Characteristics of the CEH Training Course	63
Can Web Servers be the target for hacking?	64
Wireless Networks Security: A Must Have in a Computer Network.....	65
Learning more about EC Council Certifications	66
Recognizing Security Threats: A better Way to start your CEH Online Training	

.....	68
The Best Online Training to Prepare you become a Certified Online Hacker	69
The Most sought-after Online Training Courses for Certified Ethical Hackers.....	70
Are there CEH Courses Available Onsite?.....	72
The Purpose of the Penetration Testing.....	73
Certified Ethical Hacker Online Training: Just Like in Classrooms	74
Certified Ethical Hacker Review: Self-Study Versus CEH Courses	76
Certified Ethical Hacker Series: Get Paid to Hack and Protect ...	78
A Good Certified Ethical Hacker Program Gets You Certified and Get Hired	80
Certified Ethical Hacker Schools Provide the Training Needed to Be aCEH.....	82
Preparatory Skills before Undergoing Certified Ethical Hacker Training	84
Components of a Comprehensive Certified Ethical Hacker Certification	86
Benefits of Choosing the Comprehensive Certified Ethical Hacker Online Training.....	88
Guides when Selecting the Right Comprehensive Online Certified Ethical Hacker Course	90
The Significance of Computer Forensics and Incident Handling to the Changing World	92
What to Consider When Looking for Certified Ethical Hacker	

Training Courses?	94
Knowing If It's A Comprehensive Certified Ethical Hacker Course	96
Tips in Getting the Right Comprehensive Online Certified Ethical Hacker Certification.....	98
Some Questions One Should Ask Before Choosing a Comprehensive Online Certified Ethical Hacker Online Training	100
Combating Against Corporate Espionage-Hacking Using Insiders.....	102
Council CEH	104
EC Council and Cryptography	106
Must Know about Data Loss Prevention.....	108
EC Council CEH Certifications	110
Enumeration an Essential CEH Skill.....	112
Creating Security Policies, Knowing Where to Start	114
Cyber Warfare: Hacking, Al-Qaida and Terrorism.....	116
Understanding and Learning Denial of Service Attacks.....liS EC Council Certified Ethical Hacker Certification.....	120
Must Know about Evading IDS, Firewalls and Detecting Honey Pots Training.....	122
Computer Hacking Laws: How Effective Is It Really?	124
Global Positioning System (GPS) Tacked in Detail in John Wiley & Sons Book	125
Beware of Hacking and Cheating Online Games.....	127
Hacking Email Accounts: Is it Possible?	129
Reference for Hacking Routers, Cable Modems and Firewalls:	

The Essentials	131
Footprinting: A Protection and a Risk	133
Google Hacking Gives Hackers the Opportunity to Hack	134
End the Threats in Hacking Database Servers: Shellcoder's Handbook Details How	136
Avoid from Becoming a Victim of Hacking Mobile Phones, PDA and Handheld Devices	138
Orchard's Write about Hacking RSS and Atom	140
Tools for Bluetooth Hacking	142
Becoming a Certified Ethical Hacker (CEH)	144
Do IT People Really Need a Certification Such as CEH?	145
Understanding the Concept of Buffer Overflows	147
Learning to Stop Hackers Thru CEH Books	148
A Closer Look at Computer Forensic Hacker Investigators.....	150
Taking the CEH Exam	152
Boot Camp is CEH School.....	154
What CEH Training Provides?	156
Perks of Being a CEH Certified Accredited Training Center ...	157
About the CEH Courses	159
Features of the CEH Online	161
Importance of CEH Tools.....	163
What Covers the CEH Training Course?	165
What It Means to be a Certified Ethical Hacker?.....	167
Certified Ethical Hacker Certification: Ethical Standards	169
Certified Ethical Hacker Exam: Vulnerable Systems	171
Certified Ethical Hacker Online Class: Pass on the First Take.	173
Certified Ethical Hacker Courses: Ethical Hacker or Hacker ...	174

Certified Ethical Hacker Exam Prep: Are You Prepared?	175
The Widely Used Techniques in Phishing.....	177
CEH Certification: Preemptively Preparing Computer Professionals	178
Whichever Hat You May Wear: Get Paid To Hack With CEH Certification.....	181
CEH Certification and H@cker Infiltration	184
Track down Internet Thieves with CEH Training.....	187
Computer Hacking Forensic Investigator (CHFI) Security Training	189
CertWatch.....	191

11

12

Key Elements of Physical Security

When it comes to computers, the internet and your own privacy, nothing should go and penetrate the defenses of physical security. This is very important if you want to preserve your identity as well as protect your system. By definition, physical security can be described as a measure that will help to prevent or even deter someone who wishes to access a particular location or specific information of yours.

It may even be described in the simplest ways depicting a closed door or something as highly complicated as that of a military installation. In the field of security, there are three existing elements that are essential for security measures, and those are obstacles, types of alarms and the type of security response. Obstacles may be described as measures that intend to slow down the threats or assaults to your information, but such cannot be sufficient in order to actually stop a type of serious threat.

There are also some stand alone types like locked doors, and razor wire barriers. Alarms, on the other hand, are designed to alert not just the security response team but also designed to actually unbalance your attacker. There are several

types of alarms that you may pose for your own security, but it will even be better if you combine it with a solid security response.

These security responses are the third party systems that are designed to act on your security measures are being breached. They are supposed to have the skills and the tools that are meant to immobilize or even especially eradicate your attacker and provide healing and rebuilding to any damage in your own system.

13

Proxy Server Technologies: The Lowdown

Once you find yourself connected to the web network, there are several websites out there that will offer you different kinds of features related to proxy server technologies. These features often include file-sharing and instant messaging, as well as the ability to leave comments on the profile of different users. Because of this, many schools across the country have decided to block websites that allow such access.

However, the proxy server technologies may give you a distinct technological advantage over all these restrictions. These proxy servers will allow you access to websites that have been deemed as restricted by many locations. You will then be enabled, as a user, to bypass the security-encrypted sites that are in blocked locations. Proxy server technologies will provide you with the ability to actually bypass the many network firewalls as well as filters that have been set up as safety measures for block off points.

Because of this, the proxy servers will then allow the users to surf the World Wide Web even from a blocked server. This is most commonly used in order to access sites that have popular audio and video streaming capabilities such as YouTube and MySpace. If your office has banned these websites from being accessed during work hours, you will need to figure out how to work around the proxy server technologies. If such a system is too far encrypted, you will have no other recourse but to commit to access that is outside the network that has been set up for it.

14

Multiple Ways of Scanning Your Computer

Data

Has your computer gone slow despite the beefed up in sides that you installed in it? Has it been behaving erratically for the past couple of days or weeks, refusing to follow your com mands or insisting on doing things on its own? Before you think your computer has been possessed, you should probably surmise that it may have a virus running wild and running free inside. The reason that it has a computer virus is probably because you have failed to scan it diligently.

When it comes to computer safety - in terms of both hardware and software - scanning your computer is a must. It is something that you must do on a regular basis to ensure that it is free from viruses that may steal your data or harm your system. To prevent your computer from getting yet another irritating infection, consider getting a free virus scanner.

You can get a free online scanner from websites that allow you to utilize their services in order to find infections, free of charge. You may also choose to download a free kind of antivirus product online, if you want to be protected from viruses even if you do not have an active internet connection.

There are a lot of free virus scanners, but the best ones may come at a price. You may also find a search and destroy program that will also eliminate the possibility of your computer being tracked by outside sources every time you go online to ensure maximum safety and security of your data and computer well-being.

15

Session Hijacking: Need to Know Informa tion on Protection

It has probably happened to you at one time or another: You are happily going through your business on the Internet, checking your accounts and other such stuff. Suddenly, you find yourself being logged off without your doing, or you have com mitted to some actions you do not remember doing. This simply means you have become a victim of session hijacking.

Simply put, it can be the single most irritating and scary thing that can happen to you while online - the realization that there is a physical presence out there attempting to secure your internet actions. Fortunately there are several measures

that you can implement in order to prevent this session hijacking. For one thing, you can perform security testing in many ways. On the Black Box Level (the most basic level), session hijacking is easy to address.

Session hijacking at this level is more commonly known as IP Spoofing or Internet Protocol Spoofing. In Internet Protocol Spoofing, there is a user session which is attacked even while on a protected network. The Black Box level will take care of that. If the attacker is more complicated, then session prediction will then come into play. This time, you have a method of getting the session ID of any authorized user and obtain access to the actual application.

You may then use this to retrieve the important cookies and URL, and thereby track the attacker yourself. It comes into play when it senses that there are abnormal responses to a website and even if there are stops in responses for some un known reason.

16

Social Engineering: Why You Should Be Wary

At present, there is a new budding artificially intelligent group capable of identity theft that takes advantages of the popular social engineering. This software is actually called cyber lover and works to flirt with people who are online. A lot of Russian hackers nowadays have begun to utilize the technology of social engineering in order to dupe unsuspecting internet surfers into revealing their personal information, or even luring them into going to a website that will bring their computer to the point of experiencing malware.

Such a program of social engineering works to flirt with other people online through three main avenues: by sending out emails, participating in chat conversations in chat rooms and leading you to dating websites. As it turns out, the person whom you think is expressing interest in you is not at all human. Rather, it is a program which is artificially intelligent and works to mimic the behavior of humans in a very flirtatious way.

Once the individual target begins to involve himself and flirts away with the artificially intelligent program, it will direct them to a particular blog or website that is connected to a social network. When visited by the unsuspecting user, automatic malicious codes will then be transmitted to their own computer.

Such may be very scar indeed, but the important thing to note is to always ignore

these seemingly innocent and highly flirtatious messages or heads up from people you do not know. If your privacy and safety is at stake here, the best thing you can do is to turn a blind eye to these.

17

How to Get Certified an Anti Spamming Practitioner

Spamming is one of the biggest problems bugging the cy ber world. The techniques used in spamming have become very sophisticated that companies and individuals find it increasingly difficult to prevent.

It is no wonder that spamming has been included as a ma jor topic in the certification exam for ethical hacking. If you are preparing to take a certification exam for network defense ad ministration and anti-hacking technologies, you should under stand the intricacies of spamming so you can pass the entire course work.

The best thing you can do is to attend a formal training for certified ethical hacking. Trainings are usually sponsored by the EC-Council or the International Council of E-Commerce Con sultants through its authorized training centers.

After the formal training, you can now take a Prometric test to get your certification on ethical hacking. This certification also includes your expertise on spamming techniques and spam testing. You can also self study for the exam but you need to have 2 years of experience as an IT security practitioner.

The advantage of training for the exam is you can easily grasp the underlying techniques and technologies used for spamming. You will be able to understand how spammers nor mally use bot nets or robots that perform automatic mailings and postings.

18

Once you grasp the techniques used for spamming, you will be able to spoof the process and test mail servers if spam ming activities can penetrate mailing services. You will also be capable of devising ways how to prevent spamming. Spam prevention is also included in the course work so you can implement methods such as advanced filtering, bot cancellation, bot deletion, and spam

countermeasures.

19

How Hackers perform SQL Injection and How to Fight It?

SQL injection is a technique used by hackers to discover the vulnerabilities of an SQL database and attempt to penetrate it. Usually, hackers attempt penetration through the web based log-in interface of a database.

For example, if your company has a network and you allow access to it via web based application, your legitimate users can use the log-in page on your website. They must supply a user name and password to be permitted by the system to gain access.

This log-in page is also the one being exploited by hackers. They can inject specific queries on it or commands. The SQL database on the other hand can recognize this query as legitimate so the hacker will be given access. That is why the process is called SQL injection because a hacker can inject a string of queries recognizable by the database.

Once your network has been breached, the hacker then can easily gather information and make further penetration to your system.

If you are a security administrator of an intranet, it would be best if you can attend special trainings on ethical hacking. This training can teach you the techniques used by hackers in utilizing SQL injection techniques.

Once you know how this process works, you will now be able to implement solutions on the query page of your database. This will reduce the risk of penetration and protect your intranet network from malicious hacking. It will also help you institute 20

several measures in detecting any attempt of penetration and security breach.

21

Two Methods of Training for CEH Certification Exam

There are two ways to get a certification as an ethical hacker. You can attend a formal training and proceed to take the certification exam. On the other hand, you can also self study and take the exam.

Certification for Ethical Hacking is provided by the International Council for Ecommerce Consultants. This institution is also popularly known as EC-Council.

The EC-Council assigns authorized training centers to conduct formal study and training sessions for those who want to get a certification. Once you train in one of the EC-Council's training centers, you are automatically eligible to take the exam.

After the training, you have the option to immediately sit on the exam or to defer test-taking for a later date. You must secure a certificate of attendance from the authorized training center so you can take the exam later.

The test is pro-metric so you will answer several multiple question tests. The test covers every imaginable hacking and computer security topics. It also includes spamming, spying, and creating cracks.

You can also train for CEH independent from those recommended by EC-Council. Simply study different CEH study materials and study the questions of previous exams. If you self study however, you need to send a formal application to EC Council in order to be allowed to take the exam.

22

You also need to have 2 years of experience as a systems security practitioner or systems administrator before you can take the CEH certification exam. Self study and training for the CEH is ideal if you have a complete grasp of computer security principles.

23

Understanding Viruses and Worms and the Ways to Disinfect Your Computer

The development of viruses and worms show the sophistication achieved by computer programming. Viruses and worms are pieces of applications designed specifically to destroy a computer or server system.

Viruses and worms are always attached to executable files. The methods of

distributions of these destructive programs vary. Email messages with attachments however are the most popular methods used to distribute a virus or worm.

That is why you must be wary of exe files attached to an email message. This is especially true if you received the message from an unknown sender or through forwarded messages.

Both virus and worms attach themselves to an executable command of a legitimate application. Once you open the application, the viruses will be activated and will start to destroy your computer system. Worms on the other hand can be transmitted between computers in a network. They can replicate and spawn other worms to infect other systems.

The best way to secure your network or desktop from viruses and worms is to install updated antivirus programs. Most antivirus applications will be able to detect all known viruses and applications that have virus-like behaviors.

If your system has been infected accidentally, you have to immediately disconnect your computer from the Internet. Reboot your system and run a thorough scan. Delete all applications that have been infected and again reboot your system.

24

If these steps failed, you can perform a complete reformat of your system to delete all applications on it. This will enable your computer to make a fresh start.

25

Top Two Web Application Vulnerabilities

Web applications are highly vulnerable to attacks. That's because they are constantly exposed on the Internet and can be viewed and accessed by everyone. Even if you implement security measures for your web applications, some hackers will be able to exploit its vulnerabilities. They can then proceed to hack into your system server or database once your web apps have been compromised.

PHP-created web applications are the most common target of attacks. That's because PHP is the widest programming language being used today. This does not mean that other applications created in another language are safe from

hackers.

The oldest web application vulnerability to breach the security of databases is SQL injection. This will exploit weaknesses in your web applications and inject codes or queries that may grant access to hackers. Once your web applications are compromised, your servers can suffer and your data stolen.

Remote code execution is another vulnerability that you may face. The techniques used for remote code execution is more advanced than SQL injection. The hacker will be able to trigger or activate codes in your web servers and start harvesting data.

To protect your web application from being hacked, you have to institute several layers of protection for it. Aside from the usual security access protocols, you have to deploy encrypting technologies for your web pages.

26

You should also make regular web applications security check up in order to maintain the integrity of your servers. There are many security analysts that can execute simulated attacks to test your system. This will enable you to detect if your web applications have security flaws.

27

Privacy on the Internet: Why It Pays to Be Aware

If there is one thing that you should be concerned about every time you go online, it ought to be the amount of privacy that you get on the internet. This should be your primary concern. Every time you go online, you are risking the fact that there might be people out there who will get something that belong to you - whether it is your identity, your own personal work or your financial and social details.

There are several ways by which hackers will be able to use these personal bits of information to their own advantage - which you must look at seriously because it will definitely put you at a disadvantage. First, hackers will want your financial details for the very obvious reason of stealing from you. This is very easily done by getting the details of your credit card. Every time you make an

online purchase, the security of your credit card number is challenged by the millions of hackers worldwide who are itching to use your own digits for personal gain.

Therefore, make sure that the site you purchase from has enough security to prevent these cyber robbers from getting what is yours. Second, these hackers will easily find that using your identity will be to their advantage. They can fool the people you love and trick them into giving them money or other things under the guise of your very own self. This is commonly done through email hacking. And third, they may also take credit for what is yours, so you should always watermark your images and copyright your written work to prevent it from plagiarism and cyber theft.

28

The Alarming Abundance of RFID Hacking

Actions

Companies and other kind of laboratories have been using RFID chips to conduct their day to day transactions. These RFID chips have been used as access keys - for example, many owners of vehicles have seen that they can use it to start their cars and a lot of supermarkets across the country have used these as a way to track their inventories.

Indeed, so much of today's world depends on the utility of these RFID tags that it comes as no surprise as to why there are also a lot of hacking action attempts on it. Hacking actions serve to remove the encryption that is provided by the RFID signals to protect the data that is inside it. Probably, these RFID hackers want to get into the system where they can have all the data of let's say for instance United States passports. If they are lucky, they can decode the encryption and make it less difficult for their cohorts to retrieve the vital inboard information in it.

It is scary to think that when RFID has been hacked, one could actually lose his or her own name, age, photograph and even nationality. Yet another issue in the multitude of RFID hacking actions includes the vulnerability of the system to cloning. If there is a writable area of memory on the chip, it is one hundred percent susceptible to data tampering. With this, many customers as well as corporations have decided that better and stricter measures with regard to encryption of data must be made.

1XBET

MATCHS EN DIRECT

STREAMING EN DIRECT

SUR MOBILE

Profitez du bonus!

Inscription

Par téléphone

Code *

+7

Téléphone *

912 676-78-48

Devise *

Dollar américain (USD)

Code promo (facultatif)

1SYSCASHBACK

Bonus

Bonus pour le sport

Conditions générales

Politique de confidentialité

J'ai plus de 18 ans et je confirme avoir lu et accepté les conditions générales et la politique de confidentialité de la société.

J'accepte de recevoir des offres marketing et promotionnelles par téléphone

S'inscrire

1XBET PRO

PROFESSIONAL

61%

15:31

49.77 • 1X PRO

Pro Hub

Sports

Esports

Casino

1xGames

PRIORITY AVANT-MATCH

Sport

Tout

Matches amicaux. Équipes nationales

Soon

☆

Croatie

Belgique

00 : 28 : 50

02.06.2026 (16:00)

1X2

V1 2.28

X 2.71

V2 2.256

TOURNOIS EN DIRECT

Sport

Tout

Hot

Irak. Stars League

6

☆

Hot

Russie. Coupe SFD-NCFD

1

☆

Hot

Cuba. Liga de Barrios

1

☆

RECOMMANDÉES

Casino

Tout

Pro Hub

Market Analysis

Slip Mgr.

Performance

Account

Inscription

Par e-mail

E-mail *

xxxxxxxxxx@gmail.com

Code

+7

Téléphone

000 000-00-00

Mot de passe *

WrlnPassword14

Répéter mot de passe *

WrlnPassword14

Exigences du mot de passe

Code promo (facultatif)

1SYSCASHBACK

Bonus

Bonus pour le sport

S'inscrire

1XBET

Bonus de 200 % sur le premier dépôt

Jeu responsable. Termes & conditions applicables. 18+

Profitez du bonus!

MEGABONUS POUR LE PREMIER DÉPÔT

PACK DE BIENVENUE JUSQU'À 1500 € + 150 TOURS GRATUITS

INSCRIPTION

Two Great Ways of Securing Laptop Computers

Thanks to advances in technology, more and more people have been getting laptops for themselves - some even more than one laptop per person. These laptop computers have definitely and surely started the replacement of standard desktop computers. With the falling prices of gadgets and amazing technological innovations of your time, you can definitely have a laptop computer for yourself.

But of course, when it comes to laptops security should be your prime consideration. After all, you do not want to lose all the money you invested in it. To prevent your laptop computer from being targeted by many laptop and gadget thieves, you may consider getting a notebook computer lock. It is made of durable and unbreakable material similar to that of a bicycle lock. There is a slot on the side of your laptop where one end of the lock will attach and then you may loop the cord around something secure.

It cannot be removed without the key or the combination which only you will have or know. Another thing that you can do is to invest in a laptop alarm. If by some miracle a thief manages to pry the physical lock you have for your unit, the laptop alarm will be a great way to signal to the public that something is amiss. You may download a laptop alarm on the internet and pre program it to sound off in the event that someone tries to take it from you. Follow these tips, and you are sure to keep your laptop in a very secure environment.

A Word about Sniffers and Cyber Theft

If you are an avid internet user, you have probably heard from fellow enthusiasts stories about hackers who have hawk like senses that can easily get any data that you have sent over the Internet-even if you are pretty skilled yourself. In such case, trouble may be in the way, and you will thus need the help of a network sniffer. Before any thief can create a crackdown of your encrypted data, the first thing they need to do is to capture it.

Such a process may be quite complicated for a newbie hacker, but surprisingly simple for a professional one. And for you, the dear innocent user, the best thing to do to save yourself is to utilize the help of a network protocol analyzer or a sniffer. These are hacker monitors that work overtime to analyze the network traffic and screen it from suspiciously recurring activities that are not of your doing. It works to gather clues about the kinds of data that you transmit over the internet.

If there is a pattern and the hacker captures it to satisfy their criteria, the sniffer will swoop in to intervene. It will prevent important things such as your identification names and passwords from being grabbed by others and be used for ill purposes.

For this reason alone, monitoring the network will require your utmost concentration. This is where you should consider getting the best protection that your budget will allow you because no amount of complacency will save your data from being grabbed by greedy hackers.

31

The Current State of Software Piracy and Warez

A lot of people have heard of software piracy and warez, and may even have involved themselves into it as a user or a creator. The warez usually originate from hackers who work to crack a code just for the basic thrill of overcoming a challenge. But there is another group of these misfits which you need to concern yourself with, and these are the crackers. They are also members of the hacker world who engage in software piracy, warez and most importantly, crack-and-profit activities for their own benefit.

These crackers have taken advantage of the hacker system and the skill in cracking code and thereby developing an illegal billion dollar underground economy all over the world. They thrive on different kinds of international software and of course, piracy on the World Wide Web. At the moment, hundreds of litigators, media giants and of course, the copy right holders themselves have been working actively in order to beat down these pirates and get what has been stolen from the hardworking developers of the genuine software.

There are new copyright laws that are being passed and intense international treaties that are followed in order to work together and crack down the virtual den of these underground cyber warehouses. With some help, these hundreds of thousands of cracker and hackers will be doled out with consequences they deserve. In the meanwhile, the best that you can do is to not participate in the cracking scene and instead always buy the genuine article. It will also help in avoiding you get implicated in the matter yourself.

32

Types of Computer Spying Technologies

There are many types of computer spying technologies. Some are used by malicious elements to illegally gather information on a desktop, network or server. Other spy applications however are deployed in office or home computers. The second type is designed for monitoring computer usage and activities.

If you want to become a professional ethical hacker, you need to know the methods and technologies used for computer spying. This is included in the official training for ethical hacking. A specific topic on spying technologies is also included in the actual certification exam for ethical hackers.

It is quite easy to prevent malicious spy technologies from invading a computer system. Your first recourse is to make a complete sweep of the computer registry and spot communicator applications processes. Spying technologies are also deployed through computer cookies.

Cleaning the registry and deleting cookies are normally the first steps you have to take in removing spy wares on a computer. Some spy wares however cannot be deleted by regular spy cleaner applications. You need to create special applications for such purposes. Most spy wares however are benign so you will not encounter difficulties in this area.

Ethical spying on the other hand is designed to prevent improper use of computers. It can also prevent loss of data and distribution of trade secrets. The most basic spy technologies you can use are key loggers. These are deployed on individual computers and can monitor every keystrokes made by users. There are also spy 33

technologies that capture screen shots. Incoming and outgoing email messages

can also be captured by spy applications.

34

How to Prevent System Hacking

There are numerous methods of computer system hacking. Most hacking activities attempt to steal information especially sensitive data and trade secrets. Other hackers are simple pranksters and they will try to wreck havoc on your network, computer system, or deface your website.

There are also system hacking that seeks to steal the search engine listing and ranking of your site. This is commonly used by SEOs of competing websites. The most common system hacking activities are phishing and spoofing attacks. These types of system hacking seek to gather log-in and password information from a secured web page.

Once the hackers got the password information, they will be able to penetrate the network and steal as much information from you. The information can be sold or it can be used to damage your network.

One of the best ways to prevent system hacking is to know how it works. You can take a course on ethical hacking or send your IT administrator to such training. You can also hire a system security analyst and penetrator in order to determine if your network and computer systems are vulnerable to hacking.

The security expert will simulate the methods used by hackers. Vulnerability scanning, sniffing, and security exploiting will be launched on your system. If the attempt succeeds, then this means that your system is vulnerable to attack. The consultant then can recommend measures how to prevent such attacks.

35

This could be a bit costly so your alternative is to learn how to prevent hacking. You can even take a certification exam after your training.

36

How Trojans and Backdoors Work to Wreck Havoc on Your System

Trojans and Backdoors are common programs used by hackers to gain access to a computer or network. Backdoor programs are essentially malwares and they are designed so that hackers can penetrate a computer system at the time of their choosing.

The most popular backdoor programs are Trojans. Trojans are small pieces of executable files embedded on a legitimate program. Once you download this seemingly harmless program, the Trojan will embed itself on the Rootkit of your system or on its Registry system.

Backdoors or Trojans are difficult to detect especially if your virus and computer security database is outdated. Ordinary antivirus programs will not suspect a Trojan-infected file because it will be dormant inside your computer at first contact.

Once you manually opened the infected file, the Trojan application will start to scan and open vulnerable ports in your computer. Hackers then will have a free reign on your computer and steal information.

Sometimes, if your computer is compromised by a Trojan, it can be used to infect other systems. Essentially, your computer will also become a distributor of malware without your knowledge.

It would be very difficult to remove backdoor applications and Trojans on your system. That's because they can replace an existing process and use this to open up your computer to hacks.

37

Remotely triggered backdoor applications are the most dangerous kinds of Trojans. That's because the hacker can control your computer remotely and perform spying operations.

You need to reformat your system if it has been infested with Trojans. You also need to clean your Rootkit and Registry which are the usual places where Trojans reside.

38

How to Minimize the Risk of VoIP Hacking

If you are seriously considering switching your telephony services to VoIP, then you have to understand the dangers posed by VoIP hacking to minimize risks.

Voice over Internet Protocol is a low cost and economical communication option of companies. However, if your VoiP services will be hacked you can suffer from skyrocketing communication bills.

Hackers can also tap into your VoiP services to destroy your network or gather sensitive information. It can also be used to spoof voices, distribute Trojans, and capture passwords.

In a recent security conference on VoiP hacking, IT security experts believed that hijacking access rights to VoiP will be an increasing concern for companies. As more companies migrate to VoiP, this adoption will likely attract the attention of hackers.

Hackers have a profitable interest in your VoiP services. They can hack your VoiP and sell call services to others. Malignant applications can also mimic voices and request sensitive information to your customers.

To prevent VoiP hacking, you need to implement the recommended security solutions of your provider. New devices are also equipped with security features that could effectively prevent the most common forms of VoiP hacking.

That is why it is important to deploy the latest technologies in your VoiP infrastructure and regularly check the integrity of your system. You should also try to hire a security penetra-

tion consultancy in order to test your VoiP facilities. A hacking test will determine if the security of your system is impenetrable or not. By testing your system, you can institute measures to improve its security and protect it from hackers.

40

Common Types of Web-Based Password

Cracking Techniques

There are several ways to crack passwords from web based applications. Some are crude but most methods now are very sophisticated.

To know how to fight password cracking, you need to understand the techniques used by hackers to illegally gather passwords.

First, hackers can perform brute force password cracking. This is the crudest form of hacking and it may take several weeks before the password is compromised. Essentially the hacker will simply guess the password of a user account.

Second, hackers also use dictionary attack methods to retrieve password. This involves the use of software loaded with common dictionary terms. The terms then will be supplied on the log-in authentication until the password is breached. A hybrid of dictionary attack involves the use of common words, numbers, symbols, and dashes. This is more sophisticated than brute force attacks but will take time also depending on the construction of passwords.

If you have installed excellent authentication protocols on your web applications, these methods will not work. The best way to prevent these attacks is to enforce an account lock-in feature on your log-in application. In this way, when several failed attempts have been made, the account will be automatically shut down by the system.

41

You can also add certificate authentication to your web application. This is especially useful for intranet with a web based application for log-in. What you can do is to issue certificates to users which will serve as their key in accessing their accounts. This authentication certificate is independent of the password so you will have to layers of security features for your web services and applications.

42

The Ultimate Guide towards Hacking USB Devices

Many experts of Information Technology and enthusiasts in hacking have long been thinking about how they can possibly hack a USB (Universal Serial Bus) device. For so long, not many were able to think about how they can possibly intrude on the device just until recently.

A USB Flash drive is a device that is seemingly difficult to hack because there is no programmable file that will allow auto running of a file. However, with the recent developments in computing technology, experts have found a way to hack the USB flash drive only that it can be done merely with a special flash drive device. This USB flash drive known as the U3 USB is a special drive device that is capable of being hacked.

The reason behind U3 USB capable of being hacked is because of the emulated compact disc file that is capable of being auto run. This emulated CD along with

the other auto executed file known as the flash drive is capable of being hacked. The hacker is capable to hack only the emulated CD and from there copy all the files that the flash drive has including saved documents, cache and history saved on it, e-mail files, and all relevant data that you have.

The U3 Flash drive is a little expensive compared to the ordinary device drives but because of the emulated CD (or known as the other drive letter), users can potentially maximize the use of the flash drive device. The emulated drive is capable of being used as a temporary storage of your other files and you can also use this as a way to hide or convert your important files as read only.

43

The Effective Techniques towards Better

Internet Content Filtering

With the way things have become so advanced, Internet contents have also become more difficult to regulate and control. Many web administrators have been intelligently thinking about how they can become more regulating with what can be posted and placed on the Internet.

This process is commonly referred to as the Internet Content Filtering procedure whereby the content is either allowed to be posted or blocked based on the given analysis on it. More than the source where the content came from, the Internet Content Filtering mechanism looks at the content as rather more imperative to be checked. Usually, the Internet Content Filtering is done on the e-mail messages based on the subject (vulgarity and offensiveness) and web access.

As the technology has become more advanced, the need for a more powerful and stronger Internet Content Filtering techniques are needed. Below are some of the more modernized means to filter Internet contents: a. Filtering via the attachment. Usually, attachment mode is the common carrier of malicious files. The Internet Content Filtering mechanism is looking at furthering the way attachments are being scanned and analyzed.

b. Filtering via mail header. Although mail headers are relatively easy to forge and falsify via the advanced mail tools that hackers used, it is still an effective Internet Content Filtering technique because of the highly advanced tools that e-mail programs have.

44

c. Filtering based on phrasal content. There are common phrases that malicious sites or e-mail have in their content. A better way to filter the Internet content is by setting a phrasal parameter.

45

An Explosive Revelation about hacking a Linux System

The Operating Systems are presumed to be the most difficult systems to hack and crack. More often, operating systems are shielded with highly advanced security measures that make them highly invulnerable from potential hackers. Linux Operating System which goes to the family of the Unix systems is considered one of the highly shielded operating systems that we have these days. Apparently, there has never been any recorded information whereby Linux OS was attacked by a cracker or a hacker. And if there were any hacking incidents that happened with the Linux system, the process happened from the outside because there is no apparent way that a hacker can penetrate or perform hacking or breaking inside the system. The truth about Linux is that its internal systems like its Kernels are highly shielded from within making it rather difficult for these to be hacked inside.

With the massively increasing number of institutions that are employing Linux on their computer systems, Linux manufacturers are thinking about how they can further shield and protect the system from potentially being hacked. Now, with the latest developments in Linux, it has been said the new Linux system has double firewall systems on it that makes it nearly impossible for any hacker to even penetrate on the first layer of the system because of the durable firewall system that Linux has. Apart from that, the Linux system is becoming highly improbable to be hacked because it possesses a sub system that can easily interpret hacking methods like Trojan programmable method, back door method, and possible cracking on passwords.

46

The Advantages of an Online CEH Certification

The widening technological gap between online and the offline world is seemingly inevitable. Many things that we usually do offline (meaning off the Internet) are now capable of being easily performed online (meaning on the Internet). The primary reason for this widening gap is primarily because of the comfort and ease that can be obtained out of doing it online.

This cited instance is most likely true in terms of acquiring knowledge and getting acknowledged and recognized about what you know - via the certification. More often, this certification should be done offline, however, because of the huge discomfort that offline certification brings, many people resort to having the certification online.

One of the widely becoming online certifications that we have is the CEH certification. This certification is geared at certifying the skills and knowledge of the examinee in terms of ethical hacking. Ethical hacking is learning the procedures of hacking in a legitimate and legal way. Below are some of the common advantages of online CEH certification:

- a. You can have the comfort of studying for the certification at your most comfortable laurel without being destructed or disturbed by the presence of other learners or people wanting to be certified.
- b. You can choose the best time to take the certification at your most convenient time and place. This is one of the mostly recognized advantages of online CEH certification.
- c. It is a lot cheaper and inexpensive to have the online certification compared to having it offline (this means 47 commuting to the location where the certification is going to take place.)

48

Data Recovery: A Fundamental Online

CEH Training

In the business world, they say that information is power. The loss of data in a company can mean the destruction of the whole organizational structure. This is

the reason why a lot of company leaders are investing so much in their security mechanisms in order to ensure protection in their storage of data and the transmission of raw data from one point to another.

The Certification for Ethical Hacking is fully aware of this perspective and has made sure that their programs include the safety of the data and the mechanism to recover data caused by a massive hacking and cracking activity. This training/course is fundamentally the core of all CEH trainings - the Data Recovery training.

Data Recovery training is considered to be one of the highly technical parameters of the CEH. The logical recovery data is deemed to be one of the mind boggling training lessons that one will undertake. And of course, the physical recovery of data is considered the most excruciating processes to do. The training for data recovery shall entail proper diagnosis on drives that are considered "dead and non functional" and how to recover the data from the dead drive and resurrect the device. Moreover, the data recovery training will make a learner equipped with knowledge on how to work on different OS platforms including Linux, Mac, Windows, and Unix. Along with that, the data recovery training will enhance a learner's knowledge about configuration of storage devices such as RAID enabled drives and the exchange of data via e-mail transmission.

49

The Effective Online Program to deliver the best Certified Ethical Hacker

How do we produce the best Ethical Hackers? Should we go about revisiting the trainings? Do we need to change and modify the courses being offered? Or shall we consider the time frame given to each program?

In order to deliver the best Certified Ethical Hackers, we need to undertake a few things. And one of the things that need most of the attention is the structure of every program of the CEH. An effective program to deliver the most effective and the best certified ethical hacker is the one which possesses the following characteristics:

- a. Up to date and fresh. As hackers continue to evolve so are the methods and tools that they use. If you are planning to produce the best ethical hackers then these trained people should also be immersed with the latest and up to date methods that illegal hackers use.

b. Aggressive and more powerful methods. When you develop a program to combat the problem, the solution to the problem must always be a notch higher compared to the cause.

This means that if the hacking method is highly developed and highly advanced, then you need to make sure that the online program for Certified Ethical Hackers is at par if not exceeding to the methods and tools being used by the hacker.

c. Always make sure that you experiment and deploy robust tools and methods. If you have a program that falls under the average level, then it is bound to be doomed. The only way to get out of being average is to experiment on it further and deploy the robust tools to facilitate stronger methods.

50

The Designed Online Courses for Certified Ethical Hackers

In order to become a certified ethical hacker, you will need to supplement yourself with numerous concepts and a volume of knowledge that is specifically driving at information technology, Internet and the Security threats, application systems, vast knowledge in operating systems and their differing platforms, data recovery procedure and a lot more.

What is good about these required skills is that they are made available by the governing body. The people behind the Ethnical Hacking have developed various online and offline courses to help facilitate learning. Moreover, these training courses were developed in versatile manner that tries to capture the level of expertise of every learner.

There are courses that are specifically designed for every type of learner. The training courses are designed in varied levels and they are as follows:

a. The Beginner's Level. These training courses like Fundamental Concepts of Hacking, Understanding OS and Platforms and a lot more were practically designed for those who do not have the experience in hacking but are so willing to learn. The training courses were practically drawn from the point of view of a novice.

b. The Intermediate Level. The training courses that were designed for these levels are those that are for hackers who have experience in hacking but have not

fully explored the potentials of hacking.

c. The Expert Level. The training courses for this lev-

el are practically designed for people who claim expertise in the 51

the hacking field. Training courses such as data recovery, data validation, and Intrusion Prevention are some of the courses that belong to this level.

52

Effective Online Training for an On-site

CEH

Frankly, hacking a computer system is one of the most difficult procedures to decipher. Not many people are capable of hacking a computer system but mind you, there are still people out there who are able to do that. This makes it rather alarming because there are still people who are capable of penetrating your system and can leave it openly wide for everyone else to feast.

This scenario has brought many companies to protect their own systems from any potential attack. And the only way for them to effectively do that is to train their trusted to "hack" their own system. However, this hacking procedure is given a twist as it is called as the ethical hacking.

There are many online CEH certifications and trainings that one can take should he want to earn knowledge about ethical hacking and become certified with it.

And the most effective ones are basically those which are directed towards dynamic learning in multiple platforms both in hardware and software. You see, there are Certifications for Ethical Hacking that are directed solely at a single platform. However, there are also Certifications for Ethical Hacking that are bound to be dynamic and multiple in the use of platforms. These are the best and most effective CEH trainings that one should undertake.

These online trainings may be longer than the normal and ordinary CEH trainings for obvious reason that there are just too many things to learn and understand because of the multiple platforms that the learner should be familiar with and get used to working with.

Can you hack a Site using your Web

Browser like Firefox?

Have you ever imagined on acquiring someone else's password using your ordinary web browser like Firefox or Internet Explorer? Were you able to think about how you can use a web browser in order to penetrate someone else's website?

Well, the process to hack someone else's password can somehow be described as a very strenuous work because the whole process will undertake so many steps to follow. Initially, when you think about hacking somebody else's password from your web browser you will need to locate a special file that is capable of running the cgi binary file on their end. Although this is a very strenuous work to do, there are still better ways to find this out. There are available websites that can help you out to find out if the other end is running this file from their end. You can locate the website by asking forum participants.

After this file has been located, you can then proceed on hacking the website. It is important that you already have this cgi binary file with you and make sure that you know the exact web address that you wish to hack. All you need to do is embed or add the cgi binary file that you have located at the end of the web address. You will be prompted with something else after you have accessed the web address with the cgi binary file and a little cracking on the system will allow you to openly penetrate the site. This is the technology that we have now. Things may have been far advanced and so are the means to do malicious things.

A Broad Introduction to Ethical Hacking

As they say "if you want to catch a system thief, you have to know how the thief thinks by becoming one of the thieves." And by knowing your enemy better, you will be able to have the best means to combat their attacks.

Being a hacker for a good cause is what encompasses ethical hacking. Ethical Hacking is hacking a system with due recognition and authorization in order for you to determine the possible entrance where bad hacking can happen. It is a

process of determining for yourself which part of the system is weak and able to be penetrated by black hackers (bad hackers). As an ethical hacker it is your responsibility to yield at the following end results:

- a. You must be able to hack the system without compromising the overall health of it. This means that your hacking procedure should be at all cost non destructive and should only be geared at further understanding how the system works.
- b. You must be able to come up with a diagnosis on where vulnerabilities come from. It is after all the main purpose of ethical hacking - study and determine where the system is weaker and where potential hacking may possibly come from. You need to make sure that you are able to let the management believe and understand that these unsecured spots on the system can really be the spot for hacking.
- c. You need to have intelligent suggestions and recommendations on how these vulnerable spots are capable of being patched and resolved.

55

The Realities about Hacking a Macintosh System

Macintosh is one of the highly established system manufacturers all over the world. The untarnished credibility of Macintosh in terms of reliability, durability, and dependability is unequalled in all aspects.

Now, talking about systems capable of being hacked, many consumers are thinking about the reality about Macintosh capable of being hacked. It is to be remembered that all Macintosh systems are virus-free and never has there any recorded incident that a Macintosh system has been infested by a virus. But then, hacking is all a different story; hacking never involves just putting a malicious file and allowing those malicious files destroy and ruin the whole system.

Macintosh hacking is one big milestone to happen should it becomes successful. The Macintosh system is a greatly "fire walled" system and any breakage that can happen to a Macintosh system is very unlikely to happen - not with the way these machines were designed. Apparently, since the technology happens to be very fast paced and modernized, the fact about Macintosh system being hacked is never discounted. In fact, Macintosh manufacturers have continuously been

very vigilant to any possible hacking that can happen with the system. However, as of the latest update, there has been no recorded yet, any successful attempt to hack the Macintosh system.

Macintosh is very proud and secure about the security mechanism that the system has. In fact, there has been a contest to all hackers that will authorize them to hack on the system. If one is successful to hack the Mac system then he wins. So far, 56

after many months that this Mac campaign has been launched, no one has ever made a successful attempt.

57

Internet Security: A Favorite Online CEH Course

The Certification for Ethical Hacking is a very wide and dynamic discipline. It encompasses practically about how to ensure the security of the network and the protection of the computer system against malicious hackers and crackers. This is one of the highly recommended trainings that CEH aspirants should take.

The Internet Security training is an in-depth, well researched learning platform that will be beneficial to all potential candidates of CEH. The training is geared at learning and knowing how the black hats and malicious intruders think about hacking and how they execute the process of hacking. This training reinforces the learning via the hands on or laboratory exercises which try to expose the tools and procedures used by these black hats.

The whole training about Internet Security is focused at learning the hacking process in both the network environment and stand alone systems. Primarily, every method and principle that black hats are using in their hacking activities will be dissected further. This method of learning shall then be incorporated in order to come up with a more solid method on how to combat future attacks in the system. This is going to become part of the white hat training on Internet Security.

Moreover, the training on Internet Security will draw the clear path towards how you can better assess and distinctly measure the extent of the threats of hacking in a network system. Apparently, the training shall also include how you can better 58

assess the status of a company regarding its vulnerability and exposure to potential black hats.

Become a Certified Ethical Hacker by taking the online Certification

Computing systems have become more vulnerable to all forms of malicious attacks because of the growing and progressive technology that we have. Internet users have become mature and adventurous with the way they utilize all the resources that the Internet can provide. This has made all things possible for humans.

Now, as the events turn into something, it is the best time that people get acquainted with what beset the reality - every thing and everyone is vulnerable to hackers; nothing seems to be safe in the Internet world. But the good news is that even when things have become vulnerable, there is still a way on how one can combat these potential hackers. This is done by becoming a certified ethical hacker.

A certified ethical hacker is trained to help organizations how to get prepared with the potential malicious attacks that can come their way. The certified ethical hacker is trained to think and act just like the way the hackers are. Their methods, their tools, their moves, all things that are relevant to a hacker are going to be imitated by the ethical hacker. And which system is going to be hacked? It is the company system. However, the purpose of attacking the system is far different from the purpose of the illegal hackers. The Ethical hacker does the hacking in order to determine the possible entrance where hacking can happen. And in turn, come up with a better method to combat the attack of the illegal hacker.

In order to do that, you need to be certified first. And your initial step to take the certification is to take online train-

ings and after awhile, when you are all prepared to take the certification, register in an online certification.

ers

Have you ever wondered if there are any online schools that house the minds of future ethical hackers? Or do you keep questioning yourself if this online school really helps shape the minds of the ethical hackers or is it a vision that is bound to be doomed?

Well, you may not believe it but indeed, there is a school that houses the great minds of these hackers (ethical and non ethical). It is an exclusive online school that tries to enhance and shape the great minds of the system hackers.

The online school for Certified Ethical Hackers is primarily driven by the vision to test the capabilities of these hackers in terms of methodologically penetrating a network system. The school tries to attempt on further studying how every hacker thinks prior to attacking the system and when they begin the process of attacking the whole system. In turn, when these highly trained professionals are able to extract the reasons and ways on why they attack a system, they then instill these reasons to the new breed of hackers known as the ethical hackers. However, as a twist, the ethical hackers will be taught on how these methods can help them protect and safeguard other network systems.

The online school Ethical Hackers offers various courses and training ranging from basic concepts and theories of hacking to highly complicated and difficult data recovery and Intrusion Prevention. The online school for Ethical Hackers is being governed by a group of people who are claimed experts in the field of hacking.

62

Taking CEH On-site Certification

What is CEH? Who are the people eligible to take the CEH certification? What benefits entail a certified in CEH? Where can eligible examinees take the CEH certification?

CEH stands for Certified Ethical Hacker. It is a certification that is given to any person who works in a company and is trusted by the company to penetrate the whole computing system of the organization. The person who is to undertake the penetration is given authority by the company leaders to "get inside" the system bearing the same methods to that of the illegal hacker in order to check whether the system is really capable of being penetrated. This is done by majority of companies to check the security of the system for a potential hacking.

Although the process of hacking or simply penetrating the computer system is considered illegal and has an equivalent federal punishment, when this is done upon the agreement of the company owners and the certified Ethical Hacker, this becomes legal and permissible.

Before you can be called as a certified ethical hacker, you will need to undertake a series of examinations. The Accredited Training Center is the governing and testing center that handles and facilitates the certification process. In order to qualify, you will need to acquire Internet Security experience at least in the intermediate level and have vast knowledge in various OS platforms and networking systems. There are onsite examinations being given to all potential examinees. All you need to do is to register and pay the necessary fees to be collected.

63

Understanding the Characteristics of the

CEH Training Course

What makes a person a certified Ethical Hacker? What are the prerequisites prior to becoming a certified ethical hacker? Is there any formal training that needs to be attended in order to be called a certified ethical hacker?

Being a certified ethical hacker or a CEH as they say requires quite a number of things to do before you can finally have it. Firstly, you need to undertake a CEH training course designed specifically to enhance and highlight your hacking and cracking skills. These CEH training courses have the following characteristics:

- a. The training course should be able to instill in the mind of the learner the positive effect of knowing and learning ethical hacking. This is one of the basic and most fundamental teachings that any course should emphasize.
- b. The training course should be able to direct the learner on the general overview of hacking and cracking which would be helpful in strengthening the concept of the learner about ethical hacking.
- c. The training course should be designed to allow learners understand the difference between legal from illegal hacking; ethical from unethical cracking. This will allow the learner gain a stronger foundation in ethical hacking that will presumably be used as the guiding light of every learner.
- d. The training course should teach the learner on how they can better control the

presence of a hacking incident and not be controlled by the incident itself. This is the common dilemma experienced by hacking learners. This is one aspect that should be strengthened by the designed training course.

64

Can Web Servers be the target for hacking?

With the way things are going in the information technology, do you really think that hackers are still limited with what they can do? Do you think that web servers are safe from being penetrated? Can web servers be a target of hacking? The harsh reality may be painful but yes, even web servers are capable of being hacked and to make thing worst, web servers are recently the most targeted ones. The reason why web servers are hotly being targeted is because hackers know that web servers keep so much information and details that they can use to better explore what the Internet has in possession; and for these hackers, the more information that they can capture so much the better and the best repository of huge information is a web server.

What causes web servers being hacked? Why are they easily being openly penetrated? Are there any security measures that they use?

Unfortunately, with the highly advanced pattern of thinking that these hackers have, the web server administrators are finding it rather difficult to employ all the patches that they have in order to safeguard and protect the whole server from the hackers. The tools of these hackers are highly advanced and apparently they spend so much for these tools to achieve excellence in using these. With the tools that they have, they can create a stealth mode environment while performing the hacking process that allows them to become unrecognizable and apparently invisible. This gives them the liberty to continuously do the hacking process without being interfered by a web server administrator.

65

Wireless Networks Security: A Must Have in a Computer Network

Wireless Networking is one of the fast becoming forms of networking these

days. This is considered to be the new face of Local area networking because of its ability to provide flexible, cost effective, and extensive communication means. However, with the massive growth that wireless networking has achieved, a lot of potential problems have also surfaced and one of them is the threat to security.

How do we resolve the problems of wireless network security? Are there any preventive measures that one can take in order to ensure security and protection? Can wireless networks become invulnerable with potential security threats?

Resolving a security threat whether in wireless or wired networking begins by recognizing that there is indeed a threat to the network. After having recognized that there is a threat, then you can think on how you can combat these threats effectively. And yes, there are preventive measures that one can take in order to ensure safety in your wireless network. You will need to be educated about proper protocol analysis in order for you to understand on how you can capture any possible attempts on password and username hacking.

Generally, any network can become invulnerable with any potential security threats. And yes, it can happen. The only thing that you need to do is to ensure that you have your network properly secured by having all the security preventive measures ranging from installing all the software to detect any potential cracking and hacking to positive behavior in using the network.

66

Learning more about EC Council Certifications

The EC Council or better known as the International Council of Electronic Commerce Consultants is an organization which is New York based. It is primarily a professional certification organization which has become very professional for its Ethical Hacking certification. And apart from being a certifying body for Ethical Hackers, it is also an advocate of many ethical hacking seminars and symposia.

As a governing body for IT related certification, it primarily adheres at the positively impacting aspects of computing technology such as how to recover data should any untoward incident happen like potential hacking or wrong installation that led to data loss, how to have a better and secure programming, how to do business electronically, and an overall Information Technology

Security knowledge. This is what is being encompassed by an EC Council Certification.

When you want to become a certified "white hat" person (meaning a person that does positive hacking at computer systems), all you need to do is to take a certification examination on hacking. Primarily, the certification will test your ability on how you can penetrate the system and come up with a prognosis about the possible loopholes on the system. These loopholes will be the potential spots where hacking (meaning the negative implication of maliciously penetrating a system for the benefit of the competitor) can commence.

The Ethical Hacking certification is what the EC Council is advocating. This is a common cause that a lot of concerned

Internet organizations are trying to drive these days - a worry free, non-hacked, virus-free working environment.

68

Recognizing Security Threats: A better

Way to start your CEH Online Training

If you want to become a genuine, real certified ethical hacker, you need to make sure that you have full recognition about what it means to have a better security on your system and recognize that there are threats to security. This is one of the most commonly overlooked needs towards becoming a successful certified ethical hacker.

A person who wishes to undergo certification for ethical hacking is required to undertake several learning modules in order to establish a stronger foundation about hacking. And with the dynamic trainings that one can take to fulfill the duty to become a well knowledgeable person in hacking, you can't just think about which one stands the best. However, if you are going to ask the opinions of the experts in hacking, they will all agree that all these CEH trainings are substantial and imperative. However, the most substantial lies on how you can stop hacking even before it starts. This is the training that all aspiring Certified Ethical Hackers should learn to accept.

There is an online training that is being provided to all potential Certified Ethical Hackers and this is commonly referred to as the Prevention to Intrusion. This training is basically focused on how to ensure that hacking is ended even

before it gets to start. It is very practical because it does not need human intervention for hacking to be stopped. It is an automatic system that auto executes the engine to prevent and stop almost all forms of hacking (worms, avenging employees, and viruses). What is good about this training is that damages are being contained before they get to infest the whole system which can range to about millions of company resource damages.

69

The Best Online Training to Prepare you become a Certified Online Hacker

What does the Certification for Ethical Hackers promote? What does it represent? Are there any positive implications should you become a Certified Ethical Hacker?

The Certification for Ethical Hackers is a certification given to an individual elected by the company to be trained in hacking procedure and thereby given the full authority to take a look at how the system works and its weaknesses.

Primarily, the certification gears at testing the capabilities and skills of the person in Network and Internet Security based on a neutral perspective between the industry and the manufacturing side.

This may sound very complicated and difficult but undergoing training can somehow ease the difficulty level of becoming a certified ethical hacker. You can take trainings that range from basic ethical hacking to advance ethical hacking. These trainings are all online trainings that you can acquire.

The basic ethical hacking teaches a learner the basic concepts of hacking and the difference between black hat (illegal hackers) and the white hat (legal hackers/ethical hackers). Apparently, with the advanced ethical hacking, the learner will be trained to think like both the ethical and the non ethical hackers.

At a certain point, the training will also provide methods on how the gray hat (meaning a person who is both a black and white hat) people work and the methods that they use. All of these concepts plus core learning about various operating systems and their platforms shall be unveiled and discovered when you take the online training - all best to prepare you to become a certified ethical hacker.

70

The Most sought-after Online Training

Courses for Certified Ethical Hackers

The online training courses for Certified Ethical Hackers is similarly working as the Instructor driven training courses only that with online training courses, you get to learn and acquire knowledge and concepts via the virtualized mode of teaching. It is to be noted though that with the design and structure of the online trainings, the rate of getting the right amount of knowledge has not been compromised or endangered.

One should understand that a training that is computer based or commonly referred to as the online is just another method of learning. With the online training, you are listening merely to a talking head that you see virtually rather than in person. This makes the whole training package of CEH uncompromised. While there are so many online courses that were structured to have an Instructor-driven class, there are still that remain stand out. Below are some of the well known and highly appreciated, most sought after online training courses for certified ethical hackers:

a. Advanced Forensics in Computers. This is an on-line training course that tries to dissect and understand how computer crimes are being performed by computer criminals. The Computer Forensic Experts are specifically trained to create a trace pattern to determine how and where the computer crime was committed. A background in computer forensics is required in order to study and attend this online training course.

b. Security with Application Systems. This is an on-line training course that is sought after by IT experts who are

dealing with application systems in their companies. A learner of this online training course is required to have a strong background in application software and how they are applied in the organization.

72

Are there CEH Courses Available Onsite?

The growing number of hacking incidents that are happening around is an indication that people are becoming fully aware of the massive implication of hacking and cracking. What used to be a misnomer to a lot of people has now

become a common "literature" that they can read and execute.

A lot of Internet enthusiasts and computing technology experts have seen this potential growth. This is the reason why there are so many onsite courses that are available at this time concerning ethical hacking. Ethical Hacking is a legitimate and lawful practice of hacking or penetrating a system. What is good about ethical hacking is that you get to enjoy your quench to discover the undiscovered and get a good pay for having done it. Many companies who think more about their network security go after hiring ethical hackers. This prompted for more ethical hackers to mushroom.

Many people who want to be Ethical Hackers are looking for courses that can help them enhance their hacking skills. Fortunately, just like any other IT course, there are onsite courses that one can take in order to enhance their hacking knowledge and skills. The onsite courses are practically discussing the methods and strategies that illegal hackers are doing however, the emphasis is more on how these methods can be used to help organizational entities achieve a perfectly designed security measure. Further, the skills that will be acquired with the onsite courses are structurally designed on how they can better improve the manufacturing of computer and network systems that are likely to be resistant to any hacking method or procedure.

73

The Purpose of the Penetration Testing

Have you experienced being hacked on a fully secured network system? Or have you experienced having lost all your data saved on the network and after awhile they come back intact and safe? Well, if yes, you might have experienced not being hacked but by a penetration testing.

Penetration testing is a company approved testing of the whole network system. It happens when the system is being penetrated by an ethical hacker and he tries to hack and test the vulnerability or the range of threat that a possible hacking can cause the company. This penetration testing is a mandatory testing to every company specifically those that deal with highly confidential information. Penetration testing as an intelligent method to evaluate the security and the extent of protection that the computer system has involves the following scenarios:

- a. A masqueraded black hat person attempts to get inside the system and then tries to hack the highest level of security access. The black hat person will try to

penetrate every access level and see where the soft spot lies.

b. Upon confirming the soft spot, the black hat person then creates a diagnosis on the level of security that the company has. He then evaluates the possible recommendations on how the company can better enhance their security measures.

c. When he reaches the highest level of security, the black hat person will attempt to gain access on the information residing in that section. If the attempt becomes a failure, he creates intelligent audit about what needs to be further enhanced up to that level.

74

Certified Ethical Hacker Online Training: Just Like in Classrooms

Companies and enterprises need a secure system. And with all the people out there waiting to take advantage of all the possible vulnerabilities company systems have. Companies are just getting too afraid to be infiltrated by hackers. Company systems need ample amount of security testing. They know that and they are getting strict when it comes to that. That's why there's a need for Certified Ethical Hackers. These are the people who come in and test the system according to how they see outside hackers will try to hack the system. While hacking per se is illegal, these people are authorized by the company to do it so they can fix all vulnerabilities in the system. This way they will have a more secure system.

People who want to be want to do this for a living need to get a certification. They need to be a Certified Ethical Hacker. They need to take the CEH certification exam. But for them to pass the exam they will need CEH training. Many people prefer the Certified Ethical Hacker online training. Through this type of training, they would also get instructor led training. So, they are actually like in classrooms too. Expert instructors do the training through streaming video. And they get in-depth instructions from them.

Aside from that they would also get many hours of hands on lab training. Such hands on exercises allow trainees to master things they need to pass the exam and to do their job better. They 75

will be able to master all the hacking techniques that most hackers use and guard

the company websites and systems.

76

Certified Ethical Hacker Review: Self Study Versus CEH Courses

There's a good amount of demand for security professionals. And this has made many IT individuals aim to get the Certified Ethical Hacker certification. Of course, just like any certification an exam needs to be conquered first.

In their aim to pass the exam, IT individuals are faced with a choice between taking Certified Ethical Hacker courses and doing a self study. Well, many actually opt to go for taking Certified Ethical Hacker courses. It's actually a good choice since one would be better guided by professionals. That's assuming he chooses a good CEH course, of course.

With a CEH course, people get a course outline right away. All he has to do is attend the trainings whether in class rooms or online. All the concepts and techniques needed to pass the exam will be taught. Such trainees will also get the hands on training and practice he needs for the exam.

But this could only be the optimal choice if one has enough money for CEH training. People with limited financial resources can opt to self-study. One can purchase CEH training through CDs and printed materials. These are usually cheaper than the instructor led trainings. There are even free resources on the Internet. So if one thinks he can handle studying on his own, this may be a better choice. This method will be cheaper for him. He would just have to work extra harder though.

Only the examinee can say which method is the optimal choice for him. But whichever one he chooses the important thing is to learn all the knowledge and the skills needed to pass

the exam and to be able to test and protect company systems better.

78

Certified Ethical Hacker Series: Get Paid to Hack and Protect

It's quite interesting to know that companies would hire people to try to get into their system by means of hacking. But that's what they need to do to see how secure their system is.

Security professionals do their best to use what they know about systems and about hacking to find the vulnerabilities of the company systems. But before they get hired most companies require a Certified Ethical Hacker certification. That's why many IT individuals attend the Certified Ethical Hacker series to learn as much concepts and techniques in hacking and in security.

In a Certified Ethical Hacker series, they are actually taught how to hack the systems. So while it is illegal to hack into company systems, being a Certified Ethical Hacker gives them a license to hack but only with the authorization of the companies.

After attending the CEH series, they would already be experts in sniffing passwords and gaining unauthorized access to networks and company systems. And more than that, the CEH series would also teach them how to protect the systems from this kind of exploitation.

The Certified Ethical Hacker series would help them pass the exam and to get certified. So, even if it costs them a bit of their money security professionals invest in such training. After all, the return of their investment would be quite big when they get the CEH certification and get hired.

It is, however, the responsibility of the IT individuals to use their knowledge on legal activities. The CEH series is there to

help them get certified and get hired. And if they take full advantage of the series, they will also be able to protect and secure the systems of the company they will work for better.

80

A Good Certified Ethical Hacker Program

Gets You Certified and Get Hired

Hackers seem to get better and better nowadays. That's why companies need to secure their systems more tightly. Because of this, the demand for Certified Ethical Hackers is also increasing. This is great news for IT individuals who want to do this type of practice.

To get hired, companies are looking for qualified people. This means that they need to get certified to get hired. Because of this, many IT individuals are

looking to get the CEH certification. While there are some who opt to self-study, many enroll in a Certified Ethical Hacker program to get better chances of passing the exam.

Since passing is that important to them, choosing the right Certified Ethical Hacker program is very important as well. They need to choose the best Certified Ethical Hacker program they can afford if they want to pass and get certified.

Good Certified Ethical Hacker programs may cost some money. But a good program will help IT individuals get prepared for the exam and for their jobs. Such programs are more or less comprehensive enough to teach them almost all of the tech niques and concepts that they need to know about hacking and related topics.

Penetration testing training is not just about getting the concepts. It's also about getting hands on practice. It should be something that a Certified Ethical Hacker program will provide. Trainees will get the latest techniques too so they will be able to protect the company from malicious hackers better.

81

Again, a good CEH program will let IT individuals earn all the knowledge and skills needed to pass the exam. And more than that, individuals will also be better equipped to do their jobs in testing for possible vulnerabilities in the system.

82

Certified Ethical Hacker Schools Provide the Training Needed to Be a CEH

As the need for security professionals increases, many IT individuals are encouraged to focus and strengthen their skills in security and penetration testing. Many IT individuals are enticed to get the Certified Ethical Hacker certification. As this happens, the demand for Certified Ethical Hacker trainings and course also goes up.

In response to this rising demand, the number of Certified Ethical Hacker schools has also risen. Almost all IT individuals who are interested to be a Certified Ethical Hacker would surely appreciate the availability.

Security professionals who need to get CEH trainings can get them from the CEH schools. There are CEH schools which offer classroom trainings. Many CEH schools also offer online training. Individuals have a choice between a self-paced CEH course and a scheduled training.

However, when the number gets quite big choosing a good CEH school can also be difficult. The best choice is one that can provide the best CEH training. Good Certified Ethical Hacker schools may be expensive but they will get individuals better prepared for the exam and for their future jobs.

When it comes down to actually choosing the right CEH school the individual should choose the best he can afford. The most expensive ones are not necessarily the best anyway. The important thing is to choose the school that provides the most comprehensive curriculum and training. If the individual does his best and focus on the training and on practice, he will have 83

better chances of getting certified. And when he gets hired, all his efforts would surely be worth it.

84

Preparatory Skills before Undergoing Cer

tified Ethical Hacker Training

Hacking has now been given a new name. It's not any more a name for a computer criminal alone. There is also the "ethical" hacker and this can only be proven through getting the test for Certified Ethical Hacker. But before anyone can success fully get certified, it is important to consider undergoing a Certi fied Ethical Hacker training first.

Certified Ethical Hacker training is specially created for individuals who want to undergo the certification. The goal of this is to help the applicants pass the test and finally become a Certified Ethical Hacker. For those who are planning to undergo the Certified Ethical Hacker training, there are some few things to consider.

The professional is highly advised to take the training if he is a security officer, a site administrator, an auditor, a security professional, or anyone who works with the network infrastruc ture's integrity.

Before one can undergo the tough Certified Ethical Hacker training, they should first meet certain prerequisites. They should have the desirable skills to start the training like know how on administering the Microsoft Windows 2000 Servers,

technical background on the TCP/IP, experienced file sharing with Windows and NetBIOS, and know the DHCP, WINS, and DNS. Moreover, other skills needed are knowledge on the File Permissions and NTFS, basic skills on Linux, running programs and compiling programs with Linux, and route and IP address configuration on Linux.

85

By starting with these preparatory skills, anyone can surely be able to learn fast the required skills for Certified Ethical Hacker training. The applicants are now free to choose the kind of training they desire. It could be an online training class, bootcamp, or regular classes.

86

Components of a Comprehensive Certified Ethical Hacker Certification

Being certified in the field one wants could be the most rewarding in the IT industry. Through this, one can have more knowledge as well as better future in the IT field he wants to concentrate on. Good thing there are all the certifications for everyone's IT interests. One of these is the Certified Ethical Hacker. But with the many certifications for a legal hacker, one might find it difficult to look for the comprehensive Certified Ethical Hacker certification. What most ethical hacker aspirants do not know is the existence of different components that can set aside the comprehensive from the non-comprehensive Certified Ethical Hacker certification.

A comprehensive Certified Ethical Hacker certification should be flexible for all, not only those who are real hackers. This certification should also enhance the knowledge of auditors, security officers, site administrators, security professionals, and other people who work with the network infrastructure's integrity.

Also, a comprehensive certification offers skills that will allow different professionals to understand the different weaknesses, strengths, and other vulnerabilities of the system that they are targeting. The certification should also teach professionals how to use tools, skills, and knowledge that regular hackers have in order to launch attacks. In short, the certification should train the ethical

hacker to be a real hacker.

Moreover, the comprehensive certification should be able to help different organizations learn the weaknesses of their 87

system. This can be done through launching an attack to their system while not going beyond their legal limitations. With this, they will know whether a hacker will be capable of attacking the system or not.

Getting a comprehensive Certified Ethical Hacker certification is a great choice, only if the person knows how to choose through its many components.

88

Benefits of Choosing the Comprehensive

Certified Ethical Hacker Online Training

Traditional learning is still the trend today. However, as people learn the advantages and benefits of online training, they are starting to shift to this new style of learning. Just like the comprehensive Certified Ethical Hacker training. Most people choose the online training for this course because of its many benefits.

Perhaps the most common reason why people would want a comprehensive Certified Ethical Hacker online training is its convenience. With online training, the student does not have to leave his place or work or adjust his time for the training. He can choose the time and place convenient to him without worrying about the lessons.

Another benefit of online training is its inexpensiveness. The fee for the comprehensive Certified Ethical Hacker online training is almost the same as the traditional training minus the gas expenses. So all in all, online training is more cost efficient than the offline training.

Also, having the online training at the time that the trainee wants is very possible. Online trainings are usually aimed at 1:1 learning. Therefore, the trainee has access to his course anytime, anywhere. This allows him to have more flexible time for his other things to do.

These are the common benefits one can get when choosing the comprehensive Certified Ethical Hacker online training. There are still more advantages one can find while already having the online training. But still, the person should always

89

consider his unique situation when choosing between the online or offline training since online training has its own disadvantages too. Who knows, online training might not be the best choice for a specific individual.

90

Guides when Selecting the Right Comprehensive Online Certified Ethical Hacker Course

Those who want to take the Certified Ethical Hacker certification also want to ensure that they will get certified. For this reason that many aspirants consider taking a comprehensive online Certified Ethical Hacker course. However, when they start searching for the course, they realize that the world offers many courses. So the next concern becomes how to choose among these many online courses.

Considering the learning style and course delivery will help in trimming down the Certified Ethical Hacker course choices. The aspirant ethical hacker may be convenient with electronic books. Or he may learn better with text books or other reading materials. Also, the aspirant could better learn with audio lectures that he can listen to anytime compared to having a live lecturer in front of him. Meanwhile, there are some who learn more by seeing images than listening to lectures. For them, it is best to get video-presented courses or those that are graphically demonstrated.

Also, some people may learn the Certified Ethical Hacker course more through doing. Then, the best courses for them are those with more quizzes, assignments, exams, and practical examples. Meanwhile, for those who can best learn through communicating with others, the best course is the one offering discussion groups, emails, and chat rooms.

The world really offers a lot of comprehensive online Certified Ethical Hacker courses so it is not difficult to look for one. What's more challenging is assessing all these courses and finally

decide which of them should be chosen. With these guides, the aspirant can surely get the right and the best comprehensive online Certified Ethical Hacker course for him.

92

The Significance of Computer Forensics and Incident Handling to the Changing World

Proper computer forensics and incident handling are critical to some legal cases and investigation. For legal cases, these two processes are done to analyze the computer system of the litigant or the defendant. This is also important to recover data when there is a software or hardware failure or to analyze the computer system after there was a breakin.

Computer forensics and incident handling is also helpful to get pieces of evidence against a certain employee that the organization or company wants to terminate. Sometimes, these are also used to gather data on how the computer system works and therefore make debugging, reverse-engineering, and performance optimization more effective.

However, doing all these through computer forensics and incident handling will never be effective if the pieces of evidence were not protected well.

Professionals working for computer forensics and incident handling make sure to protect the evidence. There should be no destroyed or damaged evidence or they might compromise the investigation process.

Also, these professionals want to make sure that there is no computer virus that was introduced to the computer while they are analyzing its processes. They also extract all the possible pieces of evidence and handle them properly for later use. Computer forensics and incident handling becomes more and more important as the world becomes more digitalized. Also, many organizations, businesses, and institutions are using 93

computer systems, which can be used to make crimes or harm other people. This possibility and the already done cases only prove the need for continuous practice of computer forensics and incident handling.

94

What to Consider When Looking for Certified Ethical Hacker Training Courses?

Every person planning to get certified as an Ethical Hacker knows the importance of undergoing training. With proper training, they know that they are closer to becoming Certified Ethical Hacker. However, with the many Certified

Ethical Hacker training courses available to choose from, it becomes hard to know which of these to pick. Fortunately, there are ways to know which of the training courses is the best for everyone.

The first thing to consider, is or course, the convenience of the trainee. Is online training more convenient than the class room-based? Or does having a three-day bootcamp training is better than online or classroom-based training?

Budget should also be considered when choosing an ethical hacker training course. Which of these Certified Ethical Hacker training courses is in to the budget yet offers quality training curriculum? Getting the cheapest is fine but the trainee might get better option when assessing all factors, not just the cost.

Moreover, the most important thing to consider when choosing among the Certified Ethical Hacker training courses is the curriculum. The ideal training course should have penetration testing, study of different hacker methodology, vulnerability scanning, tools for hacking, steganography, discovery of information, and countermeasures. Others in the list are hacking on the Web server, exploiting the shares, connection laundering, identity spoofing, mail spoofing, hijacking, and browser security.

95

Being a hacker is already a hard task. What more if one wants to be Certified Ethical Hacker? It is certainly more difficult than anyone can imagine. But with proper training and the right choice among the Certified Ethical Hacker training courses, anyone can study well the science of hacking the legal way.

96

Knowing If It's A Comprehensive Certified Ethical Hacker Course

The level of comprehensiveness of a certain Certified Ethical Hacker course differs from one person to another. It is difficult to define the comprehensive from not because it is a very subjective term. But there is the common or general perception of comprehensiveness, which can help in understanding the concept. This is also present in the Certified Ethical Hacker courses. So how can one know if it's a comprehensive Certified Ethical Hacker course or not?

As mentioned, there are many things that sets apart the comprehensive from not.

However, there are the common test areas like the modules of the course and the benefits one can gain from it to know which is which.

One can say that a certain Certified Ethical Hacker Course is comprehensive if it has an effective security tester methodology. The course should also aim to teach students about the different tools, methods, and techniques used by real hackers to penetrate a secured system.

Aside from these, there should also be lectures about the interesting theories on hacking offered by a comprehensive course. And finally, all these should be done within the legal limitations. The students should remain ethical while learning and after learning all the hacking skills. Ethics on hacking can be taught through introducing the principle of legal hacking.

Moreover, a comprehensive Certified Ethical Hacker course should teach different hacking concepts like methods of penetration, reconditioning of stealthy network, exploitation of 97

the remote tool vulnerabilities, Trojan hacking, wireless insecurity, and evidence removal.

Setting one's unique understanding of comprehensiveness will help also in determining the comprehensive Certified Ethical Hacker course from not. Setting the comprehensiveness is not only important but helpful too.

98

Tips in Getting the Right Comprehensive Online Certified Ethical Hacker Certification

Investing on knowledge is something that anyone does not want to take so easy. One should not only pay some hundreds or even thousands of dollars to gain knowledge. Precious time is also spent to get the most from different learning institutions. That is why people who are planning to get comprehensive online Certified Ethical Hacker certification should think and decide carefully. They should be able to get the right and their needed comprehensive online Certified Ethical Hacker certification training or they might regret it after spending some big-time dollars and time.

There are ways on how to find the right online certification program. One is to choose the right learning and certification institution. Many websites are now offering certification programs for legal hackers and one should check if the institution is legal or already accredited.

Also, checking the institution's credentials and some success stories can help in getting the right comprehensive online Certified Ethical Hacker certification. Knowing these will also inspire the person to learn and strive more to get certified. This will help him to make sure that he is getting not only the right certification program but the effective and proven too.

Choosing the right course for the Certified Ethical Hacker certification should never be missed in the list. Several courses out there are offered to the aspirants but not all of these are effective and will be helpful for the certification. The course 99

should teach all that the certification program requires so that getting certified can become closer to possibility.

Lastly, knowing the different requirements for the comprehensive online Certified Ethical Hacker certification should be assessed to know if the person is qualified or not.

100

Some Questions One Should Ask Before Choosing a Comprehensive Online Certified Ethical Hacker Online Training Being a hacker is simpler but unethical. Good thing people with a hacker's skills can now practice what they love while staying ethical too. That is through getting Certified Ethical Hacker certification. But before the aspirant rejoice a passing remark, he should first ensure to get certified. That is by enrolling in a comprehensive online Certified Ethical Hacker online training. There are a lot of online trainings in the web. So before enrolling to any of them, the aspirant should ask some questions first. Would he like it better to learn with a self-led or instructor-led online training? Some people can learn

more effectively by having an instructor who will teach them all what they need to learn and set all the deadlines for them. For people who can learn better with pressure, having an instructor-led online training is the best choice. Meanwhile, for those who are happier being left alone, setting his own rules, and working at his own pace, then a self-led online training is better. With this, one can dictate his own schedule and therefore be more flexible with his other concerns.

How much is the aspirant's budget for the online training? One might want to have the most effective and most comprehensive online Certified Ethical Hacker online training. However, he does not have the thousands of dollars for that kind of training. For those who have a short budget, they can still choose a good online training that won't require them to have a student loan. What's important is to know the modules of the online training and decide which of these offer the best.

101

Asking these two important questions will surely lead the person to the best comprehensive online Certified Ethical Hacker online training and make him closer to getting certified.

102

Combating Against Corporate Espionage Hacking Using Insiders

Along with the advancement of technology is also the increasing problems regarding computer security. For commercial organizations, the corporate espionage may be the biggest concern. But what if the hacking is done using an insider? This modus operandi can be tricky but is surely an intelligent and effective way to do corporate espionage.

Corporate espionage is done to illegally collect data that can be used against the rival corporation. Aside from using a hacker, there are still other methods to do corporate espionage like theft, dumpster diving, personnel impersonations, and intimidations.

Hackers can collect different information like the intellectual property of the company, the patents or products in progress, pricing strategies, customer information, source codes, future plans of the company, their markets, research results, latest development, technological operations, and unique manufacturing processes. All these information are critical and confidential in many companies. Once they are leaked, these could cause sales trouble or worse, downfall of the company.

Fortunately, companies can now combat against corporate espionage. Instilling to the employees the need to secure all confidential information of the company can help. The employees should also be aware of how social engineering works. Also, there should be floor marshal so that employees can report suspicious individuals. Having security software, security guards, and building security can help in combating corporate espionage as well.

103

Meanwhile, background checks of the employees will surely avoid hacking using insiders. This can be done by hiring a firm to check the identity of every employee. Security audits and assessments are helpful against corporate espionage too. Through these, the company can assess the things they do to battle against corporate espionage.

104

Council CEH

EC Council's Certified Ethical Hacker (CEH) has become one of the most recognized and fastest growing certification in the IT industry. In fact, EC-Council has reputable organizational partners that hire IT professionals to conduct authorized CEH trainings.

The long list of organizations that have IT professionals include: CISCO Corporation, Canon, Hewlett Packard, US Air Force Reserve, US Embassy, Verizon, Pfizer, FedEx, Dunlop, Supreme Court of the Philippines, Coca Cola Corporation, Quantum Research, US Military, and FBI among others. You can visit EC Council site to get the exact list of organizations that employ EC Council certified IT professionals.

EC Council specializes in invading the minds of the hackers so you can prevent them from hacking your networks. The people who work for them have Certified Ethical Hacker certification which means they have the power to stop their clients' networks from rampant hacking that is flawlessly executed by attackers. EC Council's goal towards ethical hackers is to help every organization that seeks their help in taking preemptive measures against dangerous attacks. However, every process that is done by certified ethical hackers of EC Council is grounded on legal limits.

And when you say, Certified Ethical Hacker from EC Council, they are the skilled professionals who are learned and who understand the weaknesses and strengths of attackers. Once they identify the vulnerabilities of the attackers, ethical hackers will conduct their counter attack. And since ethical hackers have authorization to probe and do counter attack for the target.

105

EC Council offers trainings, courses, materials, and other certification requirement so that candidates for CEH certification will pass the CEH examination called 312-50.

106

EC Council and Cryptography

One of Ethical Hacking and Countermeasures in taking CEH training course is cryptography. Cryptography is included in the course since the candidate for CEH (Certified Ethical Hacker) requires to learn the main components of cryptography that includes: basics of Cryptography, Public-key Cryptography,

Working of Encryption, Digital Signature, Digital Certificate, distributed.net, PGP (Pretty Good Privacy), Cryptography Attacks, Disk Encryption, CypherCalc, RSA (Rivest Shamir Adleman), RSA Attacks, MD5, SHA (Secure Hash Algorithm), SSL (Secure Socket Layer), RC5, SSH (Secure Shell), Government Access to Keys (GAK), and RSA Challenge.

The course outline of CEH training/course basically deals with the fundamentals. However, not all training partners of EC Council and other colleges and universities across the world follow the same course outline set by EC Council.

Typically, the study of Cryptography deals with the science of information security. However, since EC Council requires an in-depth understanding and practical experience from the certification candidates, the scope of Cryptography becomes wider.

The four fundamentals of cryptography are always emphasized during EC Council trainings so that candidates will acquire a kind of education that cannot be acquired from average training that other trainings provide. The four fundamentals of cryptography namely confidentiality, integrity, non-repudiation, and authentication have to be executed with extreme consideration, otherwise, cryptosystems would be disrupted.

Cryptography is an essential component of learning and understanding Ethical Hacking and Countermeasures of CEH

107

training since it protects security systems of a specific organization. Securing a system and networks is one of the utmost priorities among organization in defending their entire networks against attackers and anything that would harm their system.

108

Must Know about Data Loss Prevention

Data loss prevention is defined as a computer security for systems that determine, track, and secure data that is in use such as endpoint actions, data in motion, network actions, data at rest, and data storage.

Data loss prevention or DLP employs deep content inspection that uses centralized management framework. The DLP systems are primarily designed to

immediately detect and prevent right away any unauthorized use and transfer of information that is deemed to be confidential.

The Vendors of Data Loss Prevention Products

Vendors of DLP products refer to DLP as data leak prevention, information leak prevention, extrusion prevention system, content monitoring and filtering, and information leak detection and prevention.

Whatever vendors may call data loss prevention, one thing is for sure, DLP products are created to protect any sensitive and confidential information within an organizational system.

Understanding DLP More

Organizations have various kinds of information that are considered to be confidential and sensitive, and this is either from point of view of legal people or business people. The danger of any risk and intrusion that will come from attackers who want to gain access of confidential information is intentional transfer or sending of information to unauthorized organizations or people.

Also, there are two kinds of DLP and they are called net

work DLP and host-based DLP. Network DLP aka gateway-based 109

systems analyze network traffic so monitor and track any unauthorized entry or information transmission. On the other hand, host-based DLP normally runs on end user workstations within the organization. Host-based DLP is designed to control information that flows between users or groups. Through host-based DLP physical devices can be monitored and information can be accessed before the information has been encrypted.

DLP is essential in every organization since it has been created to serve as computer security system that will make every company protected against threats from the outside.

110

EC Council CEH Certifications

EC Council has been known in providing excellent services in defending organization's networks from hackers, in mastering the hacking technology, in training future professionals or future certified ethical hackers, and in formulating ethical hacking and countermeasures.

Yes, one of EC Council's services is to provide CEH certification to IT professionals. This is because EC Council certifications are designed in bringing and in enhancing the foundation required by Electronic Commerce and Security

Professional. For the record, EC Council Curriculum gives wide scope of skills, knowledge, and proficiency in building and managing the net works of a specific organization.

More so, security operations of organizations are also managed by ethical hackers trained in EC-Council. They are also trained to effectively employ various resources that will lead in achieving operations excellence. And so, if you are interested in pursuing a career in Ethical Hacking, you can choose from different levels of certifications that are under EC Council.

Here are the IT Security Professional Certifications available at EC-Council: Certified Ethical Hacker, EC Council Certified Security Analyst, Computer Hacking Forensic Investigator, Certified Network Defense Architect, Licensed Penetration Tester, EC Council Certified VOIP Professional, EC Council Network Security Administrator, and EC Council Certified Computer Investigator. Other certifications are also available namely certifications in Disaster Recovery and Business Continuity, Programming Certifications, Entry Level Security Certifications, Graduate Level Certifications, E-Business Certifications, 111

EC Council Security Matrix, and EC Council Continuing Education credits.

With the excellent and exemplary standards that have been set by EC Council, the candidates Certified Ethical Hacking position are extremely obliged to cope with the high standards so that the quality of services provided by EC Council will be maintained or continue to create milestones.

112

Enumeration an Essential CEH Skill

Certified Ethical Hacking course of EC Council offers wide ranging programs that will eventually develop the skills and proficiencies of the candidates for the CEH certification. Among the twenty two domains of Exam 312-50 tests for CEH certification, you will learn about enumeration.

What is Enumeration in Certified Ethical Hacking? Enumeration is a skill in certified ethical hacking. Other skills which are called domains in CEH are: ethics and legal issues, sniffers, footprinting, system hacking, Trojans and back doors, hacking web servers, web application vulnerabilities, SQL injection, hacking Linux,

Cryptography, Penetration Testing methodologies, buffer overflows, and hacking wireless networks are among the few domains.

The Objectives of Enumeration

There are four fundamental objectives of enumeration and they are: 1. To describe the enumeration steps/methods of security testing

2. To enumerate the targets of Microsoft OS

3. To enumerate the targets of NetWare OS

4* To enumerate targets of *NIX OS

Basically, enumeration extracts essential information about resources/shares that exist on the network. Enumeration extracts user names and groups that are assigned on the net work. Another function of enumeration is the extraction of last time user logged on and extraction of user's password.

113

Linux application is also relevant in Enumeration domain of CEH since through Linux application installation people can create new directory, Gzip command, tape archive file in tar format, and install applications. Scanning of NBT is also introduced in the study of enumeration.

Enumeration as a part of CEH training program will be essential since there will be study of OS history. This way, possible attacks of hacking that work in older versions of Windows OSs will be integrated to possible counterattacks using newer versions.

114

Creating Security Policies, Knowing Where to Start

Security policies are vital in every organization which is why every member of the organization/company should get themselves involved in conducting actions that concern organization data and organization network. Computer users are the ones that need more understanding toward outlining policies for the whole organization.

To start off with, the organizational management has to decide when and where to create security policies. Policies are extremely needed in every organization so that proper governance will take place. If righteous and effective security policies are executed, the company will always be protected against damages,

attacks, and threats that may come within or outside the system.

Reinforcing the security policies is also a key note that every organization should observe. Otherwise, enemies or threats from the outside will see the vulnerabilities of the entire organization and every single weakness will be used against the company.

And so, creating security policies should always be the first priority of every organization when it comes to securing their interests and in furthering the success of their organization.

In creating security policies, two significant things should be considered namely: internet acceptable use policy and email security policy. The information will come from the organization itself and it should be collected securely using policies that have been enforced by the use of technology.

115

More so, in creating security policies for the organization there should always be policy to back up data to prevent any data loss that can threaten the stability of the entire company. Creating security policies can truly be a tough job, hence involvement of knowledgeable people particularly IT professionals is indeed required.

116

Cyber Warfare: Hacking, Al-Qaida and Terrorism

The menacing effects of unsecured policies of a particular organization, and even government, can be very fatal. Cyber warfare can result from unsecured policies that are being implemented by organization called Al-Qaida. The "conjunction of 21st century internet speed and 12th century fanaticism has turned our world into a tinderbox" according to Tina Brown has also paved the way to threat to national security against Al-Qaida and terrorism.

Networked asymmetric adversaries that define Al-Qaida and its descendant affiliates internet has transformed into a sanctuary for global jihad. The global jihad has the capacity to provide advice that becomes available in real time to any militant, and this means internet is more of not just virtual memory but of a virtual university as well. And when everything falls into their right places, what

has been a virtual sanctuary and university can turn into a cyber warfare community.

Al-Qaida and the Cyber World

Al-Qaida considers the internet as a functional tool in enhancing communication, in promoting ideology, in recruiting members or believers, in getting sponsors and fundraisers, and most especially in training the newly-recruited believers.

The progeny of the internet power for Al-Qaida is in fact a cyber world that constitutes a particular kind of nervous system that has eventually developed a critical and viable structure that will allow movements in the end.

117

Therefore, to completely understand the relationship of Al-Qaida, terrorism, and even globalization you have to have an in-depth comprehension of a particularly complex organization that is a network and is comprised of networks that can be determined as both a sect and a medieval military order.

118

Understanding and Learning Denial of

Service Attacks

Basically, denial of service attacks exist but they are extremely difficult to recognize from common network activities that take place in a specified network. This extreme difficulty in distinguishing denial of service attacks is so hard to do since you can hardly identify its progress since even an indication of attack's progress can be hardly identified.

The Definition of Denial of Service Attacks

Denial of service attacks or DoS is said to be in progress when there is an attempt from the attacker to stop legitimate users of a particular network from accessing any kind of information or services. During DoS your network system or your computer is under attack, along with your network connection, you will lose access of your emails, online accounts, web sites, banking services, and other transactions that involve the use of your computer.

The Distributed DoS Attack

When you say distributed DoS attack, the attacker decides to choose your computer in attacking another computer user. The attacker primarily takes advantage of your security vulnerabilities so the attacker can eventually take in charge or manipulate your computer. As the attacker gains full control of your computer, he has gained the freedom to send/transfer huge amount of data to the website. He can also send spam messages to specific email addresses he wants. To make it simple, the term distributed DoS has been used since multiple computers, along with your computer, is being

used to launch DoS. Denial of Service attacks can hardly be stopped. However, they can be prevented by installing antivirus software, installation of firewall, and practicing good security practices.

120

EC Council Certified Ethical Hacker Certification

EC Council Certified Ethical Hacker certification requires every candidate to complete a series of steps toward their goal: the acquisition of CEH certification. To have a head start, certification track starts by attending Ethical Hacking and Counter measures course. Afterwards, the candidate has to conduct some preparations for the upcoming CEH examination. The CEH exams are called 312-50 or EC0-350. In order for the candidate to pass the examination, the candidate should undergo trainings and other ethical hacking courses. Once the candidate passed the examination, certification is given.

The EC Council Examination

Prometric is the official partner of EC Council in conducting CEH examination. For the record, Prometric is a worldwide distributor of network for computer-based services for testing. They have more than 2,500 testing centers across 180 countries. Exams at Prometric are web-based since the exam registration is available at their website.

However, the examinee should have the service of the proctor that represents EC Council Accredited Training Center. Otherwise, the candidate cannot take the CEH examination.

The listing of authorized Prometric Testing Centers is available on EC Council website. And to enable candidates to take the CEH examination, the candidate should pass the eligibility requirements. The eligibility requirements are: 1. The

candidate should have attended CEH course and it should be taken at any accredited training centers of EC Council.

121

2. But, if you don't have any training certification you are obliged to submit a proof that shows two years of information security related experiences.

3. Complete the Application Form provided by Prometric Registration.

4* Pay the certification fee that costs USD 250.

5* Go on the scheduled date of your exam by contacting the training center where you registered.

122

Must Know about Evading IDS, Firewalls and Detecting Honey Pots Training

Training programs for CEH has been recognized by the IT industry. With the quality training program that EC Council provides to every candidate who attempts to get a certification in CEH, they make sure that all skills will be learned and will be developed during the entire course of the training program. For the curriculum of the CEH training program, a particular module addresses the knowledge and skills on evading IDS, firewalls, and detecting honey pots. Therefore, to completely allow the candidate to transform their innocence into CEH proficiency a comprehensive program was developed.

Here is comprehensive program or module intended for evading IDS, firewalls, and detecting honey pots for CEH certification.

Topics 1. The introduction of intrusion detection systems

2. The identification of terminologies and their mean-

3. The components and skills under intrusion detection systems or IDS

a. The components include: IDS placement, types of IDS, ways of IDS detection, SIV or system integrity verifiers, tripwire, signature analysis, Cisco Security Agent, intrusion system, file system, and network indications, intrusion detection tools, methods to perform when IDS has been detected, evading IDS systems,

packet generators, and ways/tools in evading IDS.

123

4* Introduction of firewall, its functions and purposes, packet filtering, firewall operations, hardware and software firewalls, firewall identification, firewalking, banner grabbing, and education for other equally important components.

5* The introduction for honey pot which includes its meaning, the Honey Pot project, the types of honey pot, advantages and disadvantages of honey pot, and other issues and concerns about honey pots.

An in-depth understanding of evading IDS, firewalls and proper detection of honey pots will make the candidate more aware and more educated about what CEH is all about.

124

Computer Hacking Laws: How Effective Is

It Really?

Are the computer hacking laws effective enough? News have broadcasted that an identity of one person was stolen news such as this was not just broadcasted once and not even twice but for many times already. Often, percentages are released about the stealing of identity cases-and the figures are really high enough.

For this reason, enforcement is executing an action to resolve such incidence. But until now they are still observing whether the computer hacking laws are showing a good result against cyber crime. Cyber crime is basically cyber hacking-the attempt to void the security measures of a network or a computer. Also, hacking is performed by two kinds of people-those people who are challenged if they can do it; and those people who really use it for the purpose of destruction. It is for this reason why such case is rampant. But what really alarms the people and the authorities are the reasons why people commit such crime like for stealing or for a corporate spy.

Now, the question is if computer hacking laws are already showing a good result

to hinder the crime. Of course, the effectiveness will be measured by its deterrence. Unfortunately, it has been found out that more and more people are still attempting to do it and just avoid the crime they commit in the end. Also, there are people who commit the crime without the knowledge that they are already violating some laws, especially the sanctions that come along with the crime. But apparently, because of the existence of computer hacking laws, teens and hackers are being more controlled to stop from bringing maliciousness against people, organizations, and nations.

125

Global Positioning System (GPS) Tacked in

Detail in John Wiley & Sons Book

The Extreme Tech series of John Wiley & Sons released another book, which tackles must-have contents as well as services to clients worldwide-"Hacking GPS." Users of Global Positioning System (GPS) are aware that its manual does not explain its complete function in detail, especially when it concerns to the advanced points of the technology. The manual does not also mention the ways on how its users can tweak it, modify it, and hack it for them to maximize the function of a GPS system. But this book tackles all about these topics, especially about hacking global positioning system.

In fact, the book "Hacking GPS" provides its readers more than just the knowledge on how to maximize the function of their GPS. Essentially, this book also discusses how to bring their device and skills to more advanced levels. In addition, this book vitally fills in the missing information that should have been mentioned in the GPS manual. Hence, helping the users to get what they have actually paid for. More importantly, any possible unsafe mod for the device is vividly discussed including the precautions in the book.

To provide a gist, the following are tackled inside the Hacking GPS:

- Hardware hacks with hidden features, hacking the battery, secret codes, mounting the GPS, and making a screen protector.

- Software hacks including the hacking of the firm-

ware and hacking into one's PC Connection with a COM, USB, or GPS.

126

- Data hacks including waypoints, troubleshooting, commercial and free, creating data, and more data tricks.
- GPS Games and Hacking Geocaching

127

Beware of Hacking and Cheating Online

Games

Online games such as EverQuest, World of Warcraft, on line poker, and Second Life have conquered the computer world in an instant. But along with the rapid appearance of online games are the rapid occurrence of hacking and cheating online games as well. Numbers of online games are said to be frequently exploited and cheating in online games are getting massive. With this case, the following discussion will tackle the kinds of cheating and hacking techniques that are usually being performed in online games.

Chiefly, cheating in online games is performed by constantly changing the data files and software in some way. This normally results to the modification of the enemies' appearance wherein they can become noticeable through walls or blaze a bright color. Also, proxy servers are inserting at times some additional instructions into the data stream directly into the game server-providing cheaters with staggering aim. In many cases though, hacks are the common result of overturn engineering of the game, which end up in being circulated on the Internet.

Meanwhile, it is essential for online game developers to gain knowledge about online games hacking to keep their security against others who might pose a risk on online games they are maintaining. The fundamental of online games hacking is actually composed of six techniques:

- Crafting a bot

- Operating a proxy
- Directing memory
- Finding the future

- * Illustrating on a debugger

Among these however, bots should be given more focus by online games developers because many of the game exploits exist to build and operate them. It is also essential for online games developers to learn about controversial ways

by a particular game marker to prevent cheating.

129

Hacking Email Accounts: Is it Possible?

Surprisingly, more and more individuals today are throw ing the same questions while in the chat room. This question is "how to hack email account passwords?" Apparently, many individuals today are getting more curious or interested rather in hacking email accounts. To do this definitely, there should be some processes to follow; and more tricks to be discovered.

Before proceeding, new hackers should know that there is no any particular program that can break the password of any one's account. Some might claim that there are some password hacking programs that can be used to break someone's email account; but this claim is actually unreal. People who are using these password hacking programs only end up in disappoint ment.

What are true are the four methods that can be utilized in hacking email accounts. Below are the methods to follow to perform the hacking: o Phishing: This is considered as the most popular way to hack email account passwords. Here, a hacker will receive a mail revealing both the username and password of the victim.

o Brute Forcing: This method is almost the same as guessing the password; although here, hacker will download a password list, which will be used by the Brute Forcing.

o Keylogger: This works like Phishing although this one is a lot simpler. By installing this, one can possibly break the password of the victim, especially if the hacker has a physical access to the computer of a victim.

o Fake MSN: This is a replica of MSN messenger.

This can be downloaded and let the victim log in here, automati---

130

cally he will receive a prompt saying the Username and Password failed to match. Then, his information will be stored in a .txt file.

Reference for Hacking Routers, Cable Modems and Firewalls: The Essentials

These days, there have been some papers and books released to provide tutorials or step by step process about hacking routers, cable modems and Firewalls. Normally, these papers and books also contain diagrams, hardware schematics, source code samples, and links to software. Meanwhile, there are also some papers and books that are released to provide information on the necessary security measures, which have to be taken against some possible attacks. Such materials also present the usual vulnerabilities in a variety of prominent devices; as well, these materials illustrate weaknesses of the security in particular devices.

Specifically, hacking routers is claimed to be extensive. In fact, it has been stated that not a single router does not include some type of exploitable vulnerability. For this reason, some papers released about hacking routers used to analyze some home routers such as Linksys WRT160N, ActionTec MI424-WR, Belkin F5D8233-4v3, and D Link DIR-615.

Also, some releases about hacking cable modems tackle the mechanism that makes Internet through cable possible. Sometimes, these also reveal coverts of several prominent cable modems, which include different products. Definitely, once the cable modem was hacked, the means of exchanged of information will be hindered-interrupting the ways of communication online. So, materials that tackle about hacking of cable modem normally discuss the ways on how to clean out network ports and reveal hidden features, how to hack and change the cable modem, and tackle the significance of firmware as such.

Lastly, when it concerns to hacking firewall, some says that this trouble is not actually difficult to deal with. Anyhow, guidelines and tutorials are still provided to assure people to have an accurate reference to follow.

Footprinting: A Protection and a Risk

Today, hackers have found the most convenient way to gain information about the companies they belong to including their computer systems-footprinting. Footprinting works by allowing the hackers to know as much as they can about a system, including its ports and services, remote access capabilities, and the facets of its security.

Many are aware that during these days many companies are being threatened by hackers who can damage their system. So as a solution, they have also hired hackers to guard their systems. This is because footprinting does not solely work to attack a system; but it is also used to guard it. Logically speaking, the term "footprinting" explains its function-producing the information for someone. In fact, footprinting can also print one's favorite website.

Additionally, there is also the so-called "open-source footprinting." This is viewed as the easiest and fastest way to find information about a certain company. Examples of the open source footprinting types are the information like the addresses, phone numbers, carrying out who requests, scanning, and looking through DNS tables. Majority of this information is practically easy to obtain. And obtaining it is legal. Definitely, legal is good at all times.

What companies do not realize though is that when they post a lot of information about them on their website, hackers may use it against them. Excessive information can be too useful to hackers and can be too dangerous to companies. Companies must realize that through the use of footprinting, the vulnerabilities of a system can be revealed and can attract the risks of being exploited.

134

Google Hacking Gives Hackers the Opportunity to Hack

Hackers have a practice of searching online to find a vulnerable sensitive data and targets through the use of search engines; and this practice is termed as Google hacking. The Google Hacking Database (GHDB) is a record of inquiries that determine sensitive data. And even though Google hinders some of the recognized Google hacking inquiries, hackers are still never deterred from crawling into sites and instigating the Google Hacking Database inquiries straightly into the crawled content.

The following are the list of information that is being identified by a Google Hacking Database:

- o Reviews and server vulnerabilities

- o Error messages that have excessive information
- o Sensitive directories
- o Pages that include log-on portals
- o Pages that contain vulnerability or network data

like firewall logs

Now, the stated information above can be accessed by the hackers once they have succeeded in crawling into a vulnerable site.

So then, what are the ways to test out for Google hacking vulnerabilities?

Actually, companies can utilize a Web Vulnerability Scanner to easily determine whether their website and applications contain Google hacking vulnerabilities. A Web Vulnerability Scanner functions by scanning the entire website and automatically identifies the pages that are determined by Google hacking inquiries. However, it has to be noted that the

web vulnerability scanner that will be utilized by a company must be capable to start up Google hacking inquiries.

Now, for a company to avoid the possibility of Google hacking attacks, they should be able to remove the entire pages that are identified by Google hacking queries.

136

End the Threats in Hacking Database Servers: Shellcoder's Handbook Details How

Databases are considered as the heart of our economy. Why not? All of the personal information of many people is stored there—from the medical records, employment history, car registrations, bank accounts, pensions, down to the purchased groceries. Therefore, hacking database servers can possibly be paralyzing and crippling.

So as a solution, the four of the world's leading security experts when it comes to breaking into and securing the seven most prominent servers crafted a handbook entitled "Shell coder's Handbook." Essentially, David Litchfield, John Heasman, Chris Anley, and Bill Grindlay designed this book to help individuals in

identifying vulnerabilities, knowing how to hinder the carnage, and determining how the attacks are performed. The hackers out there are aware of these; therefore, susceptible victims of these attackers should know it as well.

Shellcoder's handbook is particularly designed for the following purposes:

- o Determine and plug up the new holes in Microsoft

- (r) SQL Server and Oracle

- o Find out the best defenses for Sybase ASE, MySQL (r), IBM's DB2 (r), and PostgreSQL

- o Discover what the attackers can possibly do

- o Learn how defense run over exploitation, trigger

abuse or stored procedure, SQL injection allow hacker access, and license escalation through the use of SQL

- o Determine vulnerabilities that are unusual to every database

137

Readers of this book gave out positive comment saying the book discussed detailed information. This also claimed to provide the information that may possibly no longer work on present systems. More importantly, the book, according to the reviews made, allow people to transform the skills above the new vulnerabilities.

138

Avoid from Becoming a Victim of Hacking Mobile Phones, PDA and Handheld De Vices

Hackers have hacked almost everything-now; they are also hacking mobile phones, PDA, and handheld devices. Hacking on these devices have surfaced just recently but to those people who are still unaware on what is really happening out there, some overviews will be provided on the

discussion below, which will be very essential to help more individuals protect their stored information in these devices.

One of the most unforgettable instance of mobile phone hacking was when Paris Hilton's cellular phone was hacked, publicizing her stored information in her device on the Internet that include the phone numbers of her prominent friends ending in a torrent of calls to everyone of them.

Certainly, mobile phone hackers have obviously discovered a hitch in the way chips are being produced. Good thing, it only applies to the models that have been released before, which utilize the Global System for Mobile communications (GSM). Additionally, hackers must have physical access to the mobile phone for three minutes at least before they can hack the device.

Unfortunately, there is still another way to hack mobile phones by installing a cellular phone hacking programs on their laptop or cell phones. Through the use of antenna, hackers can success fully steal the information stored in someone's mobile phone, especially if his mobile phone has a Bluetooth technology.

PDA and handheld devices are also susceptible now to hacking. Ironically though, one of the hot news today that is gaining more attention is the threat brought by the palm-sized 139

PDA inserted in the pocketbook of Justine Ailtel. This is claimed to be a portable

hacking device, which can automatically exploit another device.

140

Orchard's Write about Hacking RSS and Atom

Leslie M. Orchard, a certified hacker, creative technologist, and tinkerer, produced a book entitled "What are RSS and Atom Feeds." The authored book of Orchard is all about the making of cool stuff along with syndication feeds-generating technology, which can give an individual what precisely he wants. Essentially, this book tackles all about producing feeds aggregator as well as routing feeds to one's e-mail or iPod, filtering, hosting feeds, blending, and sifting them. The authors also present challenges to individuals who want to create more hacks, which she has not thought up yet.

Examples of things that can be learned through this book are the following:

- o Creating a simple feed aggregator

- o Creating additional feeds to one's buddy list
- o Tuning into well-to-do media feeds that have Bit-Torrent
- o Observing systems logs including events with feeds
- o Rubbing of feeds from outdated Web sites
- o Redirecting mailing lists into one's aggregator
- o Collecting prominent links from blogs
- o Re-issuance of feed headlines on one's Web site
- o Broadening of feeds through the use of microformats and calendar events

Additionally, this book will assist programmers, bloggers, and web developers-who already have strong background with 141

the usual RSS newsfeeds-will learn a new approach to maximize the full potential of RSS. Also, this book critically discusses the ways on how to direct RSS feeds into an e-mail inbox, bring them to a Palm device like iPod, and incorporate them into an IM systems.

Certainly, through the aid of Orchard's book, individuals can satisfy themselves with the information they need.

142

Tools for Bluetooth Hacking

Bluetooth technology is quite cool because it offers an easy way for a wide range of mobile devices to communicate with each other without the messy use of cables or wires. But there are certain threats for privacy and security in using Bluetooth.

This is the reason why many people are becoming interested in Bluetooth hacking. They want to gain a deeper understanding of Bluetooth security, the vulnerabilities in Bluetooth enabled devices and how attackers exploit them.

Some Essential Tools

There are important tools that a person can use to search out and hack Bluetooth enabled-devices, which is mostly for the Linux platform.

1. The BlueScanner searched out for Bluetooth-enabled devices and will try to extract as much information from these devices.
2. BlueSniff is a GUI-based utility for finding discoverable and hidden Bluetooth-enabled devices
3. BTBrowser is a J2ME application that can search and look around the technical specification of any Bluetooth-enabled devices. A person can even browse device information and all supported profiles and service records of each device. This application works on phones that have JSR-82 -the Java Bluetooth specification.
- 4* BT Crawler works as a scanner for Windows Mobile based devices. This application scans for other devices in range and makes service query.

These are just a few tools that people with Bluetooth enabled devices should be aware of. Should a person be much 143

concerned about Bluetooth hack attempts? There is probably not much to worry because Bluetooth devices are still in the 10 meter range. Moreover, there are also new firmware upgrades that make Bluetooth devices more secure. Also, a person can always turn off his Bluetooth when he is not using it.

Becoming a Certified Ethical Hacker (CEH)

The idea of being certified as an ethical hacker can be quite laughable for those people who are just hearing the term for the first time. Can a hacker be both ethical and certified?

The answer to this is a definite YES. Ethical hacking started out in the corporate world specifically in IBM. A CEH works to search for vulnerabilities in computer systems so that they can protect them from criminal and malicious hacker attacks. The difference between a CEH and a criminal hacker is that the former works without breaking laws or stealing data. They work because they want to uncover weaknesses using the same under-the-radar techniques that criminal hackers use.

Why think like a hacker?

Thinking like your opponent is vital to success. This is the concept behind CEH, which was first used in 1995. Certified ethical hackers must know the techniques of criminal hackers to be able to detect and stop them. Earning a CEH credential was established to be able to train IT professionals on how hackers think and act. Before the beginning of their training, CEH candidates must have two years of information security-related experience. They must also sign an agreement that they will not use their skills to learn illegal and malicious attacks.

CEH is most appropriate for managers, systems administrators and other information technology people who are involved in security. The CEH training is usually a five-day course. IT professionals can learn new ways that hackers enter the IT systems. These CEH training courses can be accessed at EC Council authorized training centers worldwide.

Do IT People Really Need a Certification Such as CEH?

Upon first hearing about Certified Ethical Certification or CEH, the first impression would be that it is intriguing and interesting. Some might even find it quite dubious because someone is getting certified to learn about hacking.

However, many IT professionals who have been trained and eventually got a CEH find it useful for their jobs especially when it involves security. Further, it is also logical to learn how hackers' mind works to be able to successfully evade or stop them.

Interested in CEH?

A person who wants to acquire a CEH must hurdle the tough examination. He can prepare for the exam by using self study materials that are available online. He can download some practice test so that he can have a feel of the real exam. There are also available training courses in videos. It will demonstrate how a person can scan, test, hack and secure IT systems. There are also lab demonstrations that give a person in depth and practical knowledge with current security system.

If you want to be more assured of quality training, you can avail of EC-Council Authorized Training Provider for online training. This training course will certainly follow the approved curriculum and shall be helpful in receiving the needed training and knowledge for certification.

Usually, the CEH certification training shows a person how to identify, counter and stop hackers to penetrate the corporate network. A person can learn how to use countermeasures

while staying ahead in terms of information security developments.

A person who is interested in IT system security can definitely find it beneficial to hold a CEH nowadays.

147

Understanding the Concept of Buffer Overflows

A buffer overflow happens when a program attempts to put more and more data in a buffer than it can't hold anymore. This condition is the most popular form of software security vulnerability. Although many software developers are aware of said security vulnerability, many attacks against legacy and newly developed applications are still happening.

Why is this so? The problem with buffer overflow is that it can occur in a wide variety of ways. This can be attributed to the error-prone strategies used to

prevent them. Moreover, buffer overflows can be difficult to discover. Sometimes even if it is discovered, it can be quite difficult to exploit. In spite of this, attackers were able to identify buffer overflows in products and components.

How is this done? A buffer overflow exploit happens when an attacker sends data to a program. This program stores the data in an undersized stack buffer, which results in information on the call stack being overwritten. Then, the data sets the value of the return pointer so that by the time the function returns, the data has transferred control to malicious code which is contained in the attacker's data.

This type of buffer overflow is quite common, but there are also other types such as heap buffer overflow, format string attack and off-by-one error. If a person is interested to learn about how buffer overflow attacks work and how he can evade them, he can do some extra reading. There are excellent books available that provide detailed information about buffer overflows.

148

Learning to Stop Hackers Thru CEH Books

There is a new strategy invading the information technology world. This is learning how to fight the enemies by knowing how they think. This is the concept behind Certified Ethical Certification. Many IT professionals are discovering the benefits of learning ethical hacking and being certified.

Why ethical hacking?

The goal of the ethical hacker is to stop criminal hackers and help an organization take preventive measures against malicious attacks. Of course, the ethical hacker works within the legal limits.

Criminal hackers have caused lots of damage in company IT systems like stealing everything valuable and even erasing their tracks. The ethical hacker must keep up with these criminal hackers by adopting an approach called "defense in depth". This means that they make penetration test wherein they test if they can penetrate their own networks and then properly make an assessment on security posture in terms of vulnerabilities and exposure.

How to learn ethical hacking?

There are various CEH books available online which a candidate can browse in a self-paced manner. There are books that are even recommended by the EC-Council website.

There are quite a number of feedbacks that some of these books come across as a not-an-easy-read book because there is no clear flow of information while some are quite overwhelmed with so much information. There are others who were able to 149

find CEH books that are quite organized, professionally done and contained only in some hundreds of pages.

A candidate who is looking for the best book that works for him may want to visit chat forum for recommendations and feedbacks for specific titles of CEH books.

150

A Closer Look at Computer Forensic

Hacker Investigators

The word hacker generally means a computer criminal who has taken over your files or worst have destroyed them. You surely wouldn't want to be called a hacker, especially if you are paid to do it legally and for a purpose.

Today, those who are employed by organization to penetrate their own networks and computer system for the purpose of finding and fixing computer security vulnerabilities are referred to as Ethical Hackers. On the other hand, those who are able to determine the person who has violated the organization's system security, when, how and what was done are referred as Computer Forensic Hacker Investigator. These two roles require certification as provided by the International Council of E-Commerce Consultants (EC Council).

The EC Council provides professional certification for Certified Ethical Hacker (CEH) and a security vendor neutral certification for Certified Hacking Forensic Investigator (CHFI). To obtain certification is either to attend training at an ATC (Accredited Training Center) or do self-study and pass the exam. If you want to become a Computer Forensics it would be best to attend the CEH class before taking the CHFI program.

Being CEH certified, you help your organization take pre-emptive measures against malicious attacks by penetrating your system itself. You try to practice catching a thief by knowing how thief thinks. Testing your systems vulnerability is being able to test how security systems work and find ways to improve them. Likewise, as a CHFI you are able to detect hack attacks and extract evidence in order to report the crime.

151

Don't let others invade your systems, detect your systems vulnerabilities. Know who your attackers or enemies and do something before it's too late.

152

Taking the CEH Exam

A Certified Ethical Hacker is one who obtains a certification of having the knowledge and tools to look into an organization's own networks and computer system for the purpose of finding and fixing computer security vulnerabilities. The ethical hacker tries to practice how to catch a thief by thinking like a thief. You need to pass the CEH exam in order to become a certified CEH. The CEH certification examination is provided by the International Council of E-Commerce Consultants (EC-Council). The examination is delivered to candidates in any of the three channels: 1. Exam 312-50: Web based 'Prometric Prime' at Accredited

Training Centers (ATC).

2. Exam ECo-350: Proctored test given at any Authorized Prometric Testing Centers (APTC) globally.

3. Exam 312-50: VUE Testing centers

CEH candidates who underwent training at any ATC are eligible to take the web based Prometric Prime exam (Exam 312-

50) at any EC-Council Accredited Training Center who will proctor the exam.

Students cannot take the exam directly through the Internet without a proctor.

Those who opted to self study can take the exam ECo-350 at the Authorized Prometric Testing Center after fulfilling the examination eligibility criteria of having 2 years experience in information security or related experience.

Candidate should

produce the voucher number to Prometric.

153

The cost to take the CEH certification exam is US\$250. The exam consists of 150 multiple choice questions and candidates from English speaking countries are given 4 hours and another 1/2 hour for non English speaking countries to

complete the examination.

The 312-50 and Eco-350 exams are identical in source and all exams leads to the certification 'Certified Ethical Hacker'.

154

Boot Camp is CEH School

Hacking is something that you do not learn from college. Hacking as a general term refers to an illegal act of gaining access to unauthorized network or computer. It is for this reason that there is no school in your undergraduate years that teach students to hack.

But hacking can be made legal only if you are an authorized Ethical Hacker. To become an Ethical Hacker is to pass the Certified Ethical Hacker exam. In as much as hacking is not taught in school, the EC Council recommends that candidates for the CEH exam attend a training course in CEH. Others who opt for self-study should present to the testing center proof of their 2 years training experience in information security measures.

Only the Accredited Training Centers of the EC Council are authorized to conduct CEH training. One good example of CEH school type training is the boot camp. Boot camps are generally done outside the location where a student resides. This is to give students time to focus on their training and prevent them from being distracted. The course outline in boot camps follows the course curriculum as released by the EC Council.

Just like in a regular school, boot camps follows a time schedules. They provide interactive and intensive learning environment, provide the learning tools and techniques of the security trade to defeat network attacks and hack-proof systems. Students are tested as to their readiness for the exam. Practice sets and lab exercises are given.

CEH school or boot camps ensures that at the end of the session, you will not leave the camp of not having learned any-155

thing. They guarantee their students the assurance of passing the CEH exam.

156

What CEH Training Provides?

Before one can take the Certified Ethical Hacker (CEH) examination, the EC Council recommends that candidates attend CEH training. CEH training covers 22 modules, that if taken in Accredited Training Centers (ATC) would have a duration of 5 days hands on training or an equivalent of 40 hours.

The CEH training includes labs exercises and practice exams with preparation sets and simulations. The training provides candidates to learn the techniques that any hacker will learn to do to infiltrate a computer system. One thing that makes the ethical hacker different from a regular hacker is that the former discovers the weaknesses prior to exploitation. Candidates for the CEH are trained on how to find these weaknesses and learn ways of testing systems security. Training also provides students the knowledge of what to do if a system is breached, if the investigation is found to have any attempted attacks and the follow up on any computer crimes.

Experienced and highly qualified instructors or security professionals lead EC Council ATCs. As you register for the CEH exam, you will only be eligible to take the exam if you have undergone training with any of the EC Council ATC. You will be given a certificate from the ATC that you have completed the course and an exam voucher for presentation to the testing center. You may need to check the list of the EC accredited training providers prior to your enrolment to a training institution.

CEH Training prepares you for the CEH exam, more so it ensures greater chance of passing the CEH exam.

157

Perks of Being a CEH Certified Accredited

Training Center

The Certified Ethical Hacker (CEH) is a professional certification that vouches for the knowledge and tools that the holder possess in terms of penetrating the weaknesses and vulnerabilities of the systems network as targeted. One of the EC Council requirements for one to be eligible to take the CEH exam is for the candidate to attend training course given by an EC Accredited Training Center (ATC). Thus, any training attended at an unauthorized training center does not make a candidate eligible to take the CEH exam. The testing centers will require candidates to show proof of official training attendance prior to exam registration.

Accredited Training Centers or Providers are the ones that deliver the hands-on instruction on security professionals. They are certified to teach the EC authorized curricula for security technologies. To be accredited as a training center, undertakes a long process of selection and screening within the EC council. EC council would have to review the training center staffing requirements and check if they are of the highest standards in terms of instructor certification, course delivery, adherence to training facility requirements, and ongoing quality commitment.

To become a member of the Accredited Training Centers is to pay a membership fee of US\$500.00. If you have other ATC under same ownership, you will need to pay USD400.00 for every additional location. To renew your membership is to pay USD250.00 per annum. There is a contract agreement between EC Council and the ATC. The following are some of the special benefits that ATC enjoys: 158

1. Access to ATC extranet Web site
2. Use of the EC-Council ATP logo
3. Authorized to conduct EC-Council official curriculum courses
- 4* ATC certificate and plaque
- 5* Discounted Exam vouchers
6. Materials used for promotions and marketing
- 7* Materials used for presentation such as CBTs, Videos, etc.

159

About the CEH Courses

Hacking is illegal if someone gains unauthorized access to computer systems but being a CEH is not. A CEH is one who has been given access by owner of the targeted system(s) or net work(s). To become a CEH is to pass the CEH exam.

There are two ways to prepare for the exam: one is through attendance to training or self study. There are EC-Council Accredited Training Centers that provides CEH courses. The CEH courses generally offer 5 days hands on training or 40 training hours. Included as well in their course program is the CEH certification exam usually given on the last day of the class.

The CEH course is open to candidates who hold position in an organization as security officers, auditors, security professionals, site administrators, and

someone who has concern as to the integrity of the network infrastructure. They should have at least two years experience in information technology, a strong working knowledge of TCP/IP, and with basic knowledge with Linux or strong working support knowledge of Microsoft XP or Vista.

CEH courses allow candidates for the CEH exam learn how to scan, test, hack and secure their own systems. They are taught as to how perimeter defenses work and lead candidates into scanning and attacking their own networks. The course also teaches candidates to learn how intruders escalate privileges and the steps to be undertaken in order to secure a system.

Some of the topics covered in the CEH courses are: 1. Developing the hacker's mind

2. Network surveying

3. Port scanning

4* System identification/OS fingerprinting

160

5* Vulnerability research and verification

6. Service identification

7* Internet application testing

8. Document grinding

9. Recognition of security issues within an organization 10. Competitive Intelligence

11. Exploiting vulnerabilities remotely

12. Examination of appropriate countermeasures to prevent malicious hacking

161

Features of the CEH Online

Prior to taking the CEH exam, the EC Council recommends that candidates attend training courses. Some people have the luxury of time to attend training classes on a 5 straight days and some prefer to train at their own paced. Online Training is training at your own paced at your own time and anywhere you want

to.

The EC Council has provided accreditation to training providers that offer online training. The training courses are designed following the approved curriculum of the EC Council. Students who prefer to have this kind of CEH Online training receives the training and knowledge that what a regular student gets from a classroom led training.

CEH Online training requires students to have Windows 2003 Server Install CD/DVD, High Speed Internet Connection, and Microsoft Internet Explorer. Students should have knowl edge in Windows Operating System, expose in the use of Linux Operating System or other Unix-based OS. They must have a grasp of the TCP/IP protocols and the desire to learn hacking and network security profession.

The CEH Online training are delivered by professional se curity instructors and generally has over 35 hours of live re cording streaming video. There are Hands on Lab exercises for students to work on. Just like training in a classroom led class provided by Accredited Training Centers, online students get the CEH examination vouchers which they may present at any Prometric testing centers worldwide.

While instructors on classroom led class are only available during classroom hours, with CEH Online training students avail 162

of the 24-hour toll free Helpdesk support for any online training application issues.

163

Importance of CEH Tools

Certified Ethical Hackers work for organizations in saving businesses from malicious hackers. They find and close the means where potential malicious hackers could exploit the organization's network, steal and destroy its data. CEH uses tools to prevent the leak of sensitive information and identify fraud or theft that may be caused by employees and customers.

Part of the CEH exam is to test CEH candidates of their knowledge of the tools used by hackers in exposing common vulnerabilities and the tools used by security professionals for implementing countermeasures. Thus it is not enough that you know the basics, but you need to show your abilities in the application of the right tools to prevent hackers from attacking network systems.

CEH Tools are provided to students who attend CEH training course. As an

Ethical hacker, you need to be alerted with threats that may significantly harm the organization's security information. Application of the CEH tools are discussed during training as to what to do if a system is breached, if the investigation is found to have any attempted attacks and the follow up on any computer crimes. With CEH Tools, students to learn on how to scan, test, hack and secure their own systems.

Some of the categories where CEH tools are included: Anti-Antivirus, Anti-Forensics, Covert Channels Tools, Fuzzers, Hex Editors, Keyloggers, Hacking Boot Disks, Remote Password Crackers, Network Recon, Passive Network Recon, Reverse Engineering Tools, Rootkits, Router Hacking Tools, SNMP Hacking Tools, TFTP Hacking Tools, Thread Protection Tools, Trojans, VoIP Hacking Tools, Web Hacking Tools, Wireless 164

Hacking Tools, and Password Cracking Dictionaries for 163 Languages.

So learn, the how's and why's on the use of those attack tools. Applying the right CEH tools would a defensive device used to your "black hat " or malicious hackers.

165

What Covers the CEH Training Course?

Organizations should give attention in ensuring that system security measures are undertaken on their system networks even before attempts of malicious hackers invade their files or destroy them. Organizations should consider sending their most trusted employees to a course that will entitle them to become Certified Ethical Hacker (CEH).

The CEH is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council). The EC-Council recommends that CEH candidates should attend CEH training course at any of the Accredited Training Center (ATC) s. They believe that attendance to the CEH training course will allow candidates to have a greater chance of passing the examinations.

There are various means to take the CEH training course. Some of these are delivered in the form of classroom led instruction, online training, training package kit, or attendance to boot camps. Normally, it takes about 5 days hands on training or 40 hours to complete a CEH training course. If the training course is conducted by an ATC, the cost of the training course includes the CEH certification exam given on the last day of class. The training course also

provides students practice exams with preparation sets and simulations. The CEH training course covers 22 modules which are discussed to students ranging from 30 minutes to 5 hours depending on the depth of the information provided. These 22 modules include: 1. Intra on Ethical Hacking

2. Footprinting

3. Scanning

4* Enumeration

5* System Hacking

166

6. Trojans and Back Doors

7* Sniffers

8. Service Denial

9. Social Engineering

10. Session Hijacking

11. Web Servers Hacking

12. Vulnerabilities in Web Application

13. Techniques on Web Based Password Cracking

14. SQL Injection

15. Wireless Networks Hacking

16. Viruses

17. Physical Security

18. Linux Hacking

19. Evading IDs, Firewalls and Honey Pots 20. Buffer Overflows

21. Cryptography

22. Penetration Testing

167

What It Means to be a Certified Ethical

Hacker?

Hacking becomes illegal if you are doing unauthorized access to network systems and files, having malicious intent of destroying them so as to avoid traceability. One means of looking into the weaknesses and vulnerabilities of your system network is to allow someone you trust to perform penetration test on your network and or computer systems by applying the tools that a regular hackers used. The person you hire to do this penetration test is known as an Ethical Hacker. To become an Ethical Hacker is to pass the Certified Ethical Hacker exam. Once certified, as an Ethical Hacker you have the authority to probe the target you found to cause harm to your systems network.

The Certified Ethical Hacker is designed for those holding positions as security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

The advantage of being a Certified Ethical Hacker is that you are legally authorized to hack malicious hackers with the use of the same knowledge and tools that malicious hackers use. As Ethical Hacker you try to catch a thief, by thinking like a thief. In this way you help organization to undertake precautionary measures or improve their systems to prevent the occurrence of being hacked in the future.

If you are looking for a job and you have the credential of a Certified Ethical Hacker, it should not be a surprise to you to know that prospective employers will do background checks or rigid personnel security investigations (PSI) for security clear-168

ances. You need to remember that hiring you as an Ethical Hacker requires lot of trust, as the company unfolds its trade secrets and you have all the liberty on hacking the company's system network without being blamed in the end.

169

Certified Ethical Hacker Certification: Ethical Standards

In groups or organizations, security is always a constant problem that is tackled again and again. There's simply no end to that as a problem, and like in the case

of medicine, where prevention is always better than cure, security demands such.

In terms of security for the websites, there are various methods available, and some are already systems-based, but these can still be exploited and defeated. The only way out of this, as the adage goes 'fight fire with fire', which now involves getting a penetration tester to hack his company to see its weaknesses. With Certified Ethical Hacker, the website's security apparatus will be checked and penetrated by the Penetration Tester or Ethical Hacker. Now any person can claim to be a Penetration Tester, but it takes a very experienced man in the business of hacking to pass the certification examination. As security is constantly under threat from hackers, a penetration tester is one that is trusted by the company to try and hack their websites or systems ethically and yet hacker-like.

With this task, there's really no wonder why the certification process is as rigid as it is when it comes to its standards. Imagine, going against security mechanisms set upon by the systems in place, and these systems are good. All hackers believe that there's a weakness in every system, and with the penetration tester certified, he can now start to find the weaknesses ethically and productively.

170

Yes, productively, as this is the kind of job that pays well and indeed the pay grade is worth the stress of having to penetrate a system that's designed to be hacker-proof.

171

Certified Ethical Hacker Exam: Vulnerable

Systems

There is no doubt that having to pass any certification examination is a hard feat to do and this is something that gets harder every year as new things are developed.

In IT, the nature of its growth is phenomenal, and because of this, certifications on this field are increasingly getting harder to pass.

There are two reasons to this. First, with the IT growing so fast and extensive, certifications like Certified Ethical Hacker is becoming more and more important.

Today, there's a growing demand for people who are well verse and certified in ethical hacking, which is fueled by the increase in hacking and number of systems vulnerable to it.

Second, the money involved in these ventures is no laughing matter and in just a matter of hours, these could disappear through effective hacking. Normally, there are many ways in which money can be stolen, but today with every bit of information being put into systems for storage, they can now be hacked.

Money doesn't always translate to its paper and coin form or in its electronic as in the case of credit and checks. Money is also in information, which whoever has it could certainly decide where the money goes, and ethical hackers make the act of hacking the companies harder.

Officially, as sanctioned by the certification agents, a person who seeks to be enrolled in the certification examination should either pass through a training session on an Accredited Training Center or through self-study. In self-study, it must first

be proven that the person is experienced for two years worth of security work, plus proper applications must be filed. After this, examination will follow.

173

Certified Ethical Hacker Online Class: Pass on the First Take

Officially, there are only one requisite demanded by the certification agents towards the exam takers. That is, they should have attended and passed a Training program from an Accredited Training Center for courses on being an ethical hacker. And that's it, and unless the 'or' part is counted as being on self-study and experience for two years, that's the only official preparation required from the exam takers.

Now after those are done, the examination would be set and taken. Of course, for any successful exam taker that would mean as the end of the story for him as hacker or as a person with no certification whatsoever.

For him it would mean jobs, even promotions and a raise, but what if he's part of the number that failed. Going through the official training program is never

enough and the exam takers need to understand this as early as possible so as to use the days as efficiently necessary.

If time is the problem or the location, then there's an on line class. Yes, there's an online class to enroll at for those who want to make sure that the certification examination is passed at their first take. It's not only pride that's at stake here, as there's also the question of money and at what is he to do without such certification.

True, the only difference between a hacker and an ethical hacker is their acts. But that doesn't leave the fact that certification is better than having nothing at all, so take the online class and buy those review materials.

174

Certified Ethical Hacker Courses: Ethical

Hacker or Hacker

In the daily grind of making security as tightly controlled as possible without raising other disruptions on the daily office job, there's still hacking to consider as a security threat.

Most companies that have already been hacked before know how these underground workers are as a menace. Trade secrets that should never be seen by the public are seen and new developments foiled by these lost information. Now there's the ethical hacker to back up the companies' systems security apparatus and they come armed to the teeth.

With such a difficult certification examination Certified Ethical Hacker is, there's really no doubt that the people who pass it are really the cream of the crop hackers.

There are numerous courses to try on this certification process and each of these courses has individual advantages that are not found on others.

In this way, the person is left to judge which course to pick, and it could very well mean either his success as an ethical hacker, or just hacker. If the certification process is no joke, then more so the courses, but this is a necessary addition without which no person would likely be able to pass, unless he's a genius.

Now it is also best to remember that this certification will mean the end of any

person's career as a hacker, which can be a criminal act in most countries. For this reason, the certification is not just given out like candy to people who profess to be former and reformed hackers.

175

Certified Ethical Hacker Exam Prep: Are You Prepared?

Preparing for the Certified Ethical Hacker examination has never been easier as there are now a number of examination preps available Online.

These can help any exam taker in making sure that he knows all there is to know about the certification examination.

Now that's a tall feat to prove, but the number of people using them through these years have been steadily increasing.

Today, there are exam preps that are given for free and some are for a price.

Caution, of course, must be exercised on both aspects, more so on the ones for free as there's always the odd-chance that the exam prep given is a dud.

There's simply no sense in experiencing the scenario where the exam taker finished his exam prep only to find out that it is full of errors. Exam preps from friends are really good to have and are mostly free from suspect, and these are especially useful when they are new.

Of course, there's also the off-chance that it could happen on exam preps being sold.

Caution is again shouted out, as to limit the amount of money saved during the certification process. Passing the certifi

cation process is the key to which former hackers and other IT personnel interested in working as ethical hackers can be successful in their field.

Without it, it is like being on the road with no car at all, while the rest of the commuters drive by on their shiny sedans.

176

Clearly, for a world where certification is something with big merit involved, it is a tough world to live in without it.

The Widely Used Techniques in Phishing

Phishing is one of the most detrimental security threats to generally of Internet users. The extent of damage that phishing can create to people is relatively massive that even lawmaker's attention has been caught by this computer crime. Phishing is the act of attempting to obtain pertinent and relevant information such as passwords, e-mail addresses, credit card information, and user name accounts among others. The act of attempting to acquire these pieces of information is of course, driven by a malicious purpose.

Usually, people are being phished without them knowing that they have already been phished with information. This ability of the phishers to masquerade as legitimate is due to the techniques that they use in phishing. Below are some of the techniques used:

- a. Phishers are able to phish for information via link manipulation. What the phishers do is they embed a link on a legitimate e-mail but the link that they embedded is the one that is not legitimate. Usually, the link will try to lead the user to a spoofed site where illegal advertisements are going to bombard the visitor.
- b. Phishers usually prevent the placement of a text which is a common filtering mechanism used by Internet administrators. Instead of the text, they replace it with graphics as the graphics are seldom being detected as a form of phishing.
- c. Phishing can also happen via forgery of websites. When you visit a spoofed site, the ordeal does not stop from there. There are highly advanced phishers who make use of JavaScript commands that change the address bar. This is fast becoming the trendiest technique used by most phishers.

CEH Certification: Preemptively Preparing

Computer Professionals

by E.S. Cromwell

Hackers can be found working their technical, backdoor, black hat magic around every Internet corner, both within computers and computer systems located far

and wide across the globe. And the computers being targeted and later infiltrated are both personal and work related. Specifically though, it is the work-based computers -whether they be for small-businesses or large companies-that are of high hacker appeal.

Why is this so? It's simply because the information within these computers is valuable and, in a sense, not all that easy to obtain. Thus, the allure is underlined and pursued - profits are there in terms of the desired information and gratification is palpable once a hack is successful and made untraceable. From the mindset of a hacker, the task of invading a network that is of corporate or large company status is a feat that any and all hackers would love to put under their accomplishment belt.

Fighting Covert Black Hats with Undercover White Hats

But, to combat and stop such black hat achievements, many individuals are wearing and wielding white hats in an undercover, yet ethical fashion. As you perhaps already know, black hat hackers are individuals who break into networks or computers and are capable of creating and/or embedding viruses. White hats, the individuals fighting against the black hats, denote a specific type of hacker that puts furtive hacking knowledge to use, yet applies it in a well-intentioned manner as to focus on securing and protecting computer systems, particularly IT computer systems.

179

These certain white hat computer professionals are best known as Ethical Hackers. But, ethical hackers, a CD you might be asking? Hacking and ethical - these two words placed next to each other? Well, yes.

Ethical Hacking Made Possible Through CEH Certification

With the surge of recent hacking activity in the world, especially on the corporate and company planes, CEH (or certified ethical hacker) individuals have been employed as to fight hacking fire with hacking fire. The thought process here is that of mental meeting or collision. EU" simply put, if you want to cease hackers from invading company systems you need to first penetrate their hacking minds and attached thought processes. And what better way to achieve this than through utilizing a professional certified hacker with proper CEH certification?

The Mission of The Professional CEH

Keeping security in mind and focusing on white hat methodologies, the aim of

professional CEH individuals is to simply safeguard an organizations computerized livelihood. Ethical hackers assist organizations, from a legal hacking-standpoint, in taking preemptive actions as to prepare for malicious black hat attacks. And this is all too important, especially in present day with how the technological world is increasingly expanding and, in turn, creating a technological dependency factor for all minor and major companies.

Certified ethical hackers are concerned about integrity and maintaining a company's network infrastructure. Through applying gained knowledge from the CEH certification any and all weaknesses or vulnerabilities can be pinpointed, tested and tweaked with through learned hacking techniques, and then, mended accordingly to maintain optimal security.

About the Author 180

If being a white hat hacker is something of interest to you, then it might be worth your while to make a career out of it through taking courses and achieving a CEH certification. Hack the right and white way, hack ethically.

181

Whichever Hat You May Wear: Get Paid To Hack With CEH Certification

by E.S. Cromwell

Are you a hacker by trade, an individual who enjoys infiltrating through backdoor computer processes? If so, and despite your hat wearing status aC"(and excuse the Dr. Seuss-esque sentence here) either being white hat, black hat, blue hat or gray hat-are you aware that there are employment opportunities for you? In fact, and probably to your surprise, there are numerous companies out there actually willing to pick you up and pay you for utilizing your hacking skills. Doubt it? Well don't, because needy companies with weak security sectors are out there and they are in quite an abundance. Truth is that employment opportunities for hackers are quite endless and companies and/or organizations are almost always in need of finding and hiring quality, intelligent and well-versed hackers to safeguard networks and counter outside attempting hacking forces.

A Mindset To Infiltrate: Both Company and Hacker Based

Thinking

Companies and organizations looking to safeguard their networks are thinking in their best and safest interests (of course), and in a very well thought out manner,

no less. What's happening on the company end is a direct hunt - companies are sniffing around and going directly to the source (hackers) to combat the source. Essentially, going to the source entails pin pointing hackers, hiring them and using their minds and experience to battle against outside hacking attempts that can literally bombard a company in an instant.

Realization of Using Hackers Against Hackers 182

The question to ask is aCCPSHow have companies come to realize such an advantageous opportunity of company-based hacker vs. self-employed hacker to better shield them?aCD The answer is quite clear cut. Companies have discerned that the notion of actually stopping hackers from invading their networks is a matter of infiltrating the hackers' minds first, seeing how they think and operate. Only here, invading minds is more so, and rather, an action of adopting minds. The difference is that companies are hiring e-minds already adept in the world of hacking, simply to do what they best - hack, break through impossible security walls and simply be, covertly effective. But, more poignantly, the intent on hiring current or once active hackers is to monitor and safeguard company networks and their online histories, shielding them from exterior and ill-intentioned hacking actions.

What Does All This Mean To You, Mr. Or Mrs. Hacker? Well, it means that if you'd actually enjoy getting paid to hack and/or work whilst hacking, you can. It's merely a matter of going through some necessary steps and attaining your CEH (Certified Ethical Hacking) Certification. As a CEH certified individual you will be required, as well as trusted, to undertake some weighted responsibilities. Of these, the main focus lies in putting forth attempts to penetrate computer systems or net works using the same approaches and methods that any normal hacker would also use. More or less, as an Ethical Hacker you will attack a security system on behalf of it owners (which is completely legal), namely targeting vulnerable points any other outside, malicious hacker could easily squeeze through. So, rather than exploit weak spots (as you would have used to do), you will find them and notify your company for instantaneous correction. Your part will be to employ preventative measures to help prepare against attemptive security breaches.

About the Author 183

So, why not put your hacking skill to use and make them, marketable? Get your CEH certification today and start, oddly enough, hacking your way to a successful career.

CEH Certification and H@cker Infiltration

by E.S. Cromwell

Ever since the advent and rise of Internet technologies, web-based loopholes and unlocked back doors have always been left open and hence, quite susceptible for most anyone to infiltrate. Specific people dubbed as aCCPSHackersaCD used and still use such passages freely and illegally. They continually enter and leave through these aCCPSdoorsaCD after doing their business, coming and going as they please - at least for the most part.

This is not saying that Hackers are left to roam about freely through cyberspace and leak through security walls, yet it is saying that only so much monitoring can actually be conducted; as it stands, a lot goes unnoticed in monitoring hacker traffic, yet, on the other hand, much is noticed, actually monitored, but is then left to transpire without halting the activity.

H@cker Classification

In hacking realms there are two types of hackers, those that initiate and instill problems and those that fix such problems. The former, are known as 'black hats' and the latter, 'white hats.' A hybrid of the two, called 'grey hats,' also exists, where both good and ill-intentions are conducted by the hacker.

Keeping this hacking subculture breakdown in mind, companies are at risk if they do not utilize employees adopting the 'white hat' persona as a Certified Ethical Hacker, or for short, CEH.

CEH Understanding & Utilization 185

Certified Ethical Hackers are a wise investment for any company looking to upgrade and fortify their Online security measures. By employing a CEH, companies are entering an agreement with such an individual to be trusted in undertaking particular penetrations of networks and/or computer systems conducting the same processes a standard hacker exercises.

Under agreement, a CEH can hack and, in lesser words, get away with it, as it is not illegal under contract between a recognized organization. As such, CEH's have complete control with little restriction, allowing such skilled tech CEH professionals to monitor weak points and penetrable spots in target computer systems of a particular organization's network.

And to take advantage of such an opportunity of CEH utilization is to directly lay and stack strengthening elements under an organizations computer framework. The benefits are apparent and the outcome is, well, safe and in the

least, safer.

H@cker Infiltration

To meet face to face with hackers and contend and safe guard well, from a company perspective, one must employ a CEH professional. Consider the mindset of a hacker and most of us would not be able to match well let alone battle on a cyberspace battlefield. Yet, CEH's can; by having a CEH under an organization's technological wing, such a mentality can be met keyboard to keyboard and challenged, simply through similar hacking knowledge and knowhow.

It's clear then, to gain ground in such a rampant cyber war where security is almost always vulnerable, companies must infiltrate the minds of hackers first, before the hackers infiltrate them. After all, to contend well against any foe, one must think as they do. And this can be done through means of hiring professional CEH's, where upon doing so can easily place any organization as victor against ongoing hacker encounters.

About the Author 186

To learn more about CEH certification research on the Web and you'll find a great amount of useful and helpful information.

187

Track down Internet Thieves with CEH Training

by Shannon Margolis

A Certified Ethical Hacker is one who knows how thieves and hackers work. The best way to catch a thief is to act like a thief, and to be able to get inside their minds, to prevent them from hacking your network. The best way to find out if your network is secure is to attack it in just the same manner that a hacker would.

The goal of an ethical hacker is to help take preemptive measures against malicious attacks. This is done by attacking the system while staying within legal limits. The philosophy behind this stems from the practice of catching a thief by thinking like one. This has proved crucial as technology advances and the dependency on technology increases.

The CEH training course will put the students into an interactive environment where they will be shown the techniques to test, hack, and then secure their systems. This CEH course at <http://jwww.unitek.com/trainingjceh.php> is lab intensive, and gives the students in depth knowledge and experience with the

most current, and essential security systems.

Students in this CEH certification course will be taught how perimeter defense works, and they will then be taught how to scan and attack their networks. No real networks will be compromised in this course though. The students are taught how intruders break into networks, and the steps they can take to secure a system. Students will be taught about several different attacks, such as DDos attacks, and virus creation. They will also 188

be taught, in this intensive five day course, about intrusion detection, social engineering, and policy creation.

The intensive CEH training course is composed of twenty two modules, each teaching a different aspect of CEH. The course begins with lessons in ethics and legality, followed by web application vulnerabilities, foot printing, web based password cracking techniques, and scanning. The course continues with an SQL injection module, enumeration, hacking wireless networks, and system hacking. Next comes the very things that nearly anyone who uses the internet is concerned about, including a virus and worms module, then Trojans and backdoors, physical security, sniffers and Linux hacking. There is even a module about cryptography. There are lots of intensive, hands on laboratory work in this course.

After the course, students will be prepared to sit for the certification exam, which after passing, they will be certified ethical hackers. This course would significantly benefit security officers, system administrators, and really anyone who is concerned about the security and integrity of their network.

About the Author

Shannon Margolis

IT Marketing Coordinator www.unitek.com/training 189

Computer Hacking Forensic Investigator

(CHFI) Security Training

by Shannon Margolis

Computer hacking forensic investigation, or CHFI, is detecting and properly extracting evidence from hacking incidents. This is done in order to not only report the crime, but also conduct the audits necessary to prevent any future attacks.

The information gathered in these investigations is crucial in cases dealing with disloyal employees, industrial espionage, e mail fraud, web page documents, and

computer breakins among many other types of computer hacking crimes. Computer hacking forensic investigators can use many different methods to discover and recover data from a computer system.

Law enforcement, military personnel, security professionals, system administrators, legal, banking, and government agencies, as well as many other computer related professionals can all benefit from CHFI training. The course will provide students with the knowledge and skills needed to identify an intruder and gather the evidence needed to prosecute them. It is highly recommended that students take the CEH course before taking the CHFI course. The student will learn everything from the history of the field, to the laws involved, the actual process involved in investigating computer hacking crimes, as well as the proper procedures to follow when doing so. The CHFI training will cover the necessary steps to take, the software involved, and the newest techniques for investigation available.

190

Students will also learn how these criminals operate, thus coining the phrase, "To catch a thief, you have to think like one." There is also an entire module that teaches the students how to properly act as an effective expert witness, from preparing to testify, the technical and legal aspects of being an expert witness, and how to testify during both direct and cross examinations. There is a laboratory module that will teach students to know their way around a forensic computer lab, as well as the equipment necessary to run a computer hacking forensic investigation laboratory. The final module deals with computer forensics in action.

There are three steps necessary to become certified in computer hacking forensic investigation. CHFI certification requires a focused student who is ready and eager to learn and achieve. Students must complete all of the required course work, and then prepare for the examination. If you are ready to challenge yourself and perform the tasks of only a select few, then the CHFI course will propel into the dark and mysterious world understanding the criminal mastermind.

For more information on obtaining your Computer Hacking Forensic Investigator (CHFI) Security Training please visit http://jwww.unitek.com/training/descs/chfi_bootcamp.php.

About the Author

Shannon Margolis

CertWatch

by Jason Sprague

It is time to take a look at the certifications that will be the buzz words for the year. This is not a list of which certifications will be the most popular; it is a list of the certs that will experience major continued growth or have their first growth spurt. Keep in mind that these are expert predictions and educated guesses, but are not scientifically based.

1) Prosoft Learning's CIW Foundations

OK.. I am going out on a big limb with this one. Several years ago, the CIW certification program was growing rapidly and the future of this program looked very bright. Then, as quickly as the buzz started, it all came crashing down when Prosoft Learning announced financial difficulties and later went through a failed attempt at integration with Trinity Learning. In late 2004, the company underwent management changes and spent too much of 2005 worrying about their NASDAQ status instead of reinvigorating their certification program. However, I believe that this is the year that they will turn the ship around. It shouldn't be too difficult considering the fact that this is still the best certification option for webmasters. Foundations is their entry level title and should experience the most growth in the coming year. If CompTIA updates their antiquated i-Net+ certification and the 2 companies renew their broken partnership, the CIW Foundations title will experience significant additional growth.

2) Cisco's CCIP

I believe that the Cisco Certified Internetworking Professional certification will grow quite a bit this year, but mostly in developing countries who will be expanding their infrastructure 192

leading to the need for more service providers. This certification is also attractive because it shares 1 exam with the CCNP cert and another exam with the CCVP cert.

3) Wireless#

Although plagued by early problems, wireless networking has become a reliable solution for SOHO environments and for other applications, and the market has created a need for technicians that can install and troubleshoot wireless networks. To the best of my knowledge, CWNP is currently the only certification

vendor offering vendor neutral wireless certifications. In October 2005, Planet3Wireless announced the release of Wireless# which is an entry level title. Because it is affordable, only requires 1 exam, and there is a market need, this cert should take off in 2006.

4) EC Council's CEH

Yes, security is still a hot topic and will remain so as long as there are losers that have nothing better to do than harm others. EC Council's Certified Ethical Hacker cert is rapidly gaining steam and the reason for this is a slightly different approach to security - learn how to hack your systems in order to prevent others from doing it.

5) CompTIA's Linux+

Linux+ is an entry-level Linux certification and a popular stepping stone on the way to other Linux qualifications such as LPIC and Red Hat certifications. As long as the popularity of higher level Linux certifications continues to increase, Linux+ will follow suit.

6) Cisco's CCVP

VOIP and IP telephony have been around for a little while, but it is beginning to appear that this will be the way of the future when it comes to voice communications. While being a fairly new title, the Cisco Certified Voice Professional certification is simply the most logical choice in this rapidly growing arena.

7) LPI's LPIC 1

193

Over the last couple of years, the Linux Professional Institute's LPIC 1 certification has gained credence and growing market recognition. This is partially due to a general increase in the popularity of Linux and Linux certification. It is also due to the fact that LPI's program fills a void that none of the other vendors do; an intermediate Linux credential with a reasonable price tag.

8) Microsoft's MCITP

The Microsoft Certified IT Professional designation is part of Microsoft's new certification paradigm that was recently announced. The MCTS will essentially replace the MCSA and MCSE designations for future tracks, and for that reason, it should have instant success. We will see this certification take off when Windows Vista is launched and the new certification track is released.

9) Microsoft's MCTS

Like the MCITP, the Microsoft Certified Technology Specialist designation is another new title that has been added to Microsoft's revamped certification program. It will essentially be the equivalent of the current MCP title and for that reason, it will eventually become the most popular certification available.

About the Author

For more information and free study tools for IT certifications and careers, visit MC MCSE - a world leader in helping people get certified the right way.

Additional learning materials can be found at TechTutorials.net - a massive directory of free computing tutorials.

INDEX'

194

A

ability 13, 65-6, 163, 177

Abundance of RFID Hacking Actions 4, 28

Accredited Training Centers, see ATC

aggregator 140

agreement 62, 144, 185

AI-Qaida 7, 116-17

alarms 12, 124

application systems 50, 70-1

applications 15, 23-5, 41, 134, 142, 147, 163, 172, 192 based 19, 40-1
spy 32-3

APTC (Authorized Prometric Testing Centers) 152

aspirants 90-1, 98, 100

ATC (Accredited Training Centers) 62, 120, 150, 152, 154, 156-7, 161,

165, 171, 173

attachments 23, 43

attackers 12, 15, 104, 107-8, 118, 136, 147, 151

attacking 59, 61, 87, 118, 159, 187 attacking network systems 163

attacks 25, 34, 40, 54, 57, 59, 61, 87, 113-14, 118, 131, 133, 136, 147,
179, 187 [2]

counter 104 attendance 21, 159, 165

auditors 84, 86, 159, 167

Authorized Pro metric Testing Centers (APTC) 152

auto 42, 68 automatic system 68

B

backdoors 36, 188
Beware of Hacking and Cheating Online Games 8, 127
black hats 57, 178, 184
Bluetooth devices 143
Bluetooth-enabled devices 142
Bluetooth Hacking 8, 142
Bluetooth technology 138, 142
book 2-3, 125, 131, 136-7, 140-1, 148 boot camps 9, 154, 165
bats 127-8
break 129, 178, 182 brute 40
Brute Forcing 129
budget 30, 94, 100
buffer overflows 8, 112, 147, 166

C

195

cable modems 131
candidates 105-6, 112, 120, 122-3, 148-9, 152, 154, 156-7, 159, 161, 165
candidates Certified Ethical Hacking position 111 career 110, 174, 180, 183, 193
Caution 175
CEH (Certified Ethical Hacker) 2-3, 5-9, 48-50, 59, 62-3, 68-70, 82, 94-6, 104, 144-6, 150, 156-7, 159, 167, 184-5, 187-9 [22] CEH books 148-9
CEH certification 46, 62, 78, 80, 105, 110, 112, 120, 122, 179-80, 183, 187
CEH Certification 9, 178-9, 181, 184
CEH certification exam 22, 74, 153, 159, 165
CEH certification examination 152
CEH certification research 186
CEH certification training 145
CEH Certified Ethical Hacker 4
CEH courses 159
CEH exam 120, 152, 154-7, 159, 161, 163
CEH Exam 9, 152
CEH examination 105, 120
CEH On-site Certification 5, 62

CEH Online training 161
CEH schools 82, 154
CEH series 78
CEH tools 163
CEH Tools 9, 163
CEH training 48, 63, 68, 74, 76, 82, 106, 144, 156, 163, 165, 187
CEH Training 5, 9, 63, 156, 165, 187
certification 5-6, 8-9, 17, 21, 46-7, 59-60, 66, 68-9, 86, 98, 110, 145, 150, 152-3, 173-4, 191-3 [9]
popular 193
certification agents 171, 173 certification candidates 106 certification exam 17, 21, 32, 35, 188
certification examination 66, 169, 171, 173, 175 certification fee 121
Certification for Ethical Hackers 69
Certification for Ethical Hacking 21, 48, 57 certification gears 69
certification institution 98 certification online 46 certification option, best 191 certification paradigm 193
certification process 62, 169, 174-5
certification programs 98-9, 191 revamped 193
right 98
right online 98
certification requirement 105
196
certification track 120, 193 certification vendor 192
Certifications for Ethical Hacking 52
Certified Ethical Certification 145, 148
Certified Ethical Hacker, see CEH
certified ethical hacker certification 9, 76, 78, 82, 90, 98, 100, 104, 169 certified ethical hacker courses 9, 76, 96, 174
Certified Ethical Hacker Exam 9, 171
Certified Ethical Hacker Exam Prep 9, 175 certified ethical hacker examination 175
Certified Ethical Hacker Online Class 9, 173
Certified Ethical Hacker Online Training 6, 74, 88
Certified Ethical Hacker programs 6, 80
Certified Ethical Hacker Review 6, 76
Certified Ethical Hacker Schools 6, 82 certified ethical hacker series 6, 78
Certified Ethical Hacker training 82, 84-5 certified ethical hacker training courses 94-5
certified ethical hackers 5, 49-50, 61, 70, 74, 80, 104, 110, 144, 179, 185, 188
certified ethical hacking 17, 112, 182 certs 191-2
cgi 53

cheating 127-8
cheating online games 8, 127
CHFI (Computer Hacking Forensic Investigator) 9, 110, 150, 189-90
CHFI certification 190
CHFI training 189 choice 76, 82, 87, 90
optimal 76
choosing 7, 36, 80, 82, 88-9, 94, 98, 100
Cisco Certified Internetworking Professional certification 191
Cisco Certified Voice Professional certification 192
CIW certification program 191 class 70, 159, 161, 165 classrooms 6, 74, 161, 165 **code execution, remote 25**
combat 49, 54, 57, 59, 65, 102, 178, 181 comfort 46
Common Types of Web-Based Password Cracking Techniques 5, 40 companies 2, 17, 19, 28, 38, 48, 52, 62, 71-4, 78-80, 102-3, 114-15, 133-5, 168-9, 181-2, 184-5 [9]
large 178 needy 181
companies migrate 38
companies renew 191 company systems 59, 74, 77-8 components 6, 86-7, 106, 122-3, 147 comprehensive certification 86
Comprehensive Certified Ethical Hacker 6-7, 96
197
comprehensive Certified Ethical Hacker certification 86-7
Comprehensive Certified Ethical Hacker Certification 86 comprehensive Certified Ethical Hacker online training 88 comprehensive online Certified Ethical Hacker certification 98-9 comprehensive online Certified Ethical Hacker online 100
Comprehensive Online Certified Ethical Hacker Online 7, 100
comprehensiveness 96-7
computer 4, 6, 12, 14, 16, 23-4, 32, 36-7, 70, 72, 92, 118, 124, 129, 154, 178 [1]
laptop 29
computer crimes 70, 156, 163, 177 computer criminals 70, 84, 150
Computer Data 4, 14
Computer Forensic Hacker Investigators 8, 150 computer forensics 70, 92-3, 150, 190
Computer Forensics and Incident Handling 7, 92
computer hacking crimes 189 investigating 189
computer hacking forensic investigation laboratory 190
Computer Hacking Forensic Investigator, see CHFI Computer Network 65
computer security 102, 108 computer security principles 22 computer security system 109 computer security topics 21 computer spying technologies 4, 32 computer system hacking 34
computer systems 23, 32, 34, 36, 45, 52, 57, 62, 66, 73, 92-3, 133, 144, 150, 152, 178 [5]

protecting 178

Computer users 114, 118 computer virus 14, 92

concepts 8, 50, 63, 69-70, 76, 78, 80, 96, 144, 147-8 contend 185

cost 54, 65, 78, 80, 88, 94, 153, 165 countermeasures 94, 106, 110, 120, 160 courses 6, 50-1, 61, 72, 90, 98, 105, 173-4, 180

comprehensive online Certified Ethical Hacker 90 onsite 72

crack 21, 31, 45

crackers

31, 45, 57

cracking

40, 53, 63, 72

crawling

134

crime 93, 124, 150, 189

cyber 124

Cromwell 178, 181, 184 cryptography 7, 106, 112, 166, 188 cryptosystems 106

cybertheft 4, 27,30 cyber world 17, 116

198

D

data loss prevention 7, 108 data recovery 5, 48, 51, 61 data recovery training 48 databases 19, 25, 136

computer security 36 defeat network attacks 154

defending organization's networks 110

deploy 38, 49 designations 2

Designed Online Courses for Certified Ethical Hackers 5, 50 destroy 23, 38, 163, 165

devices 38, 42, 48, 125, 131, 138-9, 142 difficult systems 45

DLP 108-9

host-based 108-9

DLP products 108

DLP systems 108 domains 112

DoS 118

drive, flash 42

durable firewall system 45

E

E-Business Certifications 110

EC 156-7

EC council 157

EC Council 66, 104-6, 110-12, 120, 122, 150, 154, 156-7, 161, 192

EC-Council 17, 21, 104, 110, 144, 152, 165

EC Council ATCs 156

EC Council CEH Certifications 7, 110

EC Council certifications 110

EC Council Certifications 6, 66

EC Council Certified Computer Investigator 110

EC Council Certified Ethical Hacker certification 120

EC Council Certified Ethical Hacker Certification 8, 120

EC Council Certified Security Analyst 110

EC Council Examination 120

EC Council Network Security Administrator 110

EC Council Security Matrix 111 employees 92, 102-3, 163, 184 emulated CD 42

encryption 28, 106

enemies 54, 114, 127, 148, 151

English speaking countries 153 enrolling 100

Entry Level Security Certifications 110 enumeration 7, 112-13, 166, 188

Enumeration in Certified Ethical Hacking 112

199

espionage, corporate 7, 102-3 ethical 61, 63, 69, 96, 100, 144, 179 ethical hacker aspirants 86

Ethical Hacker Certification 7

ethical hacker training 94 comprehensive Certified 88

ethical hackers 6, 9, 21, 32, 54, 59, 61, 66, 69, 72-3, 104, 148, 152-4, 167-9, 173-5, 179 [10]

aspirant 90

aspiring Certified 68 authorized 154

best 49

best certified 49 best Certified 49

best comprehensive online Certified 91, 101 certification examination Certified 174 certified 62-3

comprehensive Certified 96-7 comprehensive online Certified 90, 100 hiring 72

online school 61

potential Certified 68 professional 32

real certified 68

right comprehensive online Certified 98

ethical hacking 5, 17, 19, 21, 32, 34, 46, 48, 52, 54, 57, 63, 68, 72, 110, 148 [4] advanced 69 basic 69

understanding 106

Ethical Hacking and Countermeasures 106, 120

Ethical Hacking and Countermeasures of CEH 106 ethical hacking certification 66

ethical hacking courses 120

evading IDS systems 122 evidence 92, 189

exam 17, 21, 74, 76-8, 80-2, 90, 112, 120-1, 145, 150, 152-4, 156, 159, 192

exam preps 175

exam registration 120, 157 exam takers 173, 175

examination 62, 120, 145, 152-3, 156, 160, 165, 172-3, 190

examinee 46, 76, 120

experience 17, 22, 50, 106, 121, 152, 173, 181, 187, 191 experiment 49

experts 42, 68, 70, 78 extraction 112

extrusion prevention system 108

F

200

feedbacks 148-9 file system 122

files 42, 53, 84, 150, 165, 167

binary 53

filtering 5, 43-4, 108, 140

Firefox 5, 53

firewall systems, double 45 firewalls 8, 119, 122-3, 131 flirts 16

focus 82, 128, 154, 178, 182 footprinting 8, 112, 133, 165 formal training 17, 21, 63 function 112, 123, 125, 133, 147 fundamentals 106

G

GAK (Government Access to Keys) 106 game 127-8

GHDB (Google Hacking Database) 134

Global Positioning System, see GPS

Global System for Mobile communications 138

Google hacking 134-5

Google Hacking 8, 134

Google hacking attacks 135

Google Hacking Database (GHDB) 134

Google hacking vulnerabilities 134

Government Access to Keys (GAK) 106

GPS (Global Positioning System) 8, 125

GPS system 125

Graduate Level Certifications 110 graphics 177

groups 31, 61, 90, 109, 112, 169

growing certification, fastest 104 growth 171, 191

guard 75, 133 guides 7, 90-1

H

H@cker Infiltration 9, 184-5

hack 5-6, 8-9, 25, 36, 38, 42, 45, 53-5, 73-4, 78, 125, 127, 131, 134, 169, 180-2 [10]

hack attacks 150

hack email account passwords 129 hack-proof systems 154

Hacker Online Training 7 hacker system 31

hackers 19, 25, 27, 30-1, 34, 36-40, 45, 49-50, 61, 64, 129, 133-4, 144-5, 173-5, 178-82, 184-5 [22]

criminal 144, 148 illegal 59, 62, 69, 72

201

legal 86, 98 potential 45, 59 real 86, 96

regular 86, 156, 167

hacking 5, 7-8, 45-6, 50, 52-5, 57, 61-6, 68-9, 72-3, 78, 94-6, 102-4, 124-5, 154, 167-9, 181-3 [19]

malicious 19, 160 online games 127 potential 54, 62, 66

Hacking actions 28

hacking activities 57, 179 com man system 34

hacking database servers 8, 136 hacking email accounts 8, 129

hacking incidents 45, 63, 72, 189 hacking knowledge 72, 185 hacking methods 45, 49, 72 hacking mobile phones 8, 138 hacking procedure 52, 54, 69 hacking process 57, 62, 64 hacking routers 8, 131

Hacking RSS and Atom 8, 140

hacking skills 72, 96, 181, 183 hacking techniques 75, 127

learned 179 hacking test 39

Hacking Tools 164

Hacking USB Devices 5, 42

hacking wireless networks 112, 188

handbook 136

handheld devices 8, 138 hats, white 178, 184

hiring 103, 168, 181-2, 185 honey pots 123, 166

detecting 122

hours 74, 153, 156, 161, 165, 171 houses 61

I

IDS 122

evading 122-3

IM systems 141

incident handling 7, 92-3

individuals 17, 76, 78, 80-2, 84, 129, 136, 138, 140-1, 178-9 infiltrate 156, 181, 184-5

infiltrating 181-2

information security 106, 121, 152 inject 19

insiders 7, 102-3

instill 61, 63

202

institutions 21, 45, 92, 98 instructor 70, 74, 76, 100, 161 instructor certification 157 instructor-led online training 100

International Council of E-Commerce Consultants 17, 150, 152, 165 internet 4, 12, 15, 23, 25, 27, 29-30, 43, 46, 50, 59, 64, 76, 114, 116, 127 [4]

Internet content 43-4

Internet Content Filtering 43 internet organizations 67

Internet Protocol Spoofing 15

Internet Security 5, 57, 62, 69

Internet Security training 57

Intra on Ethical Hacking 165 intrusion detection systems 122 intrusion system 122

invading 32, 104, 178, 182

invading company systems 179 investigation computer hacking forensic 189-90 personnel security 167

iPod 140-1

J

jihaad, global 116

jobs 74, 80-2, 115, 145, 167, 170, 173

K

Key Elements of Physical Security 4, 12 keyboard 185

Knowing 7, 96, 98, 114

knowledge 46, 48, 50, 52, 62, 70, 76, 78, 81, 84, 86, 98, 110, 124-5, 145, 156-7 [10]

knowledgeable person 68

L

laptop 29, 138 laptop alarm 29

laws, computer hacking 8, 124

learner 46, 48, 50, 52, 63, 69, 71
learning 6, 46, 50, 57, 66, 88, 96, 106, 148 learning ethical hacking 63, 148
Learning to Stop Hackers 8, 148 legal cases 92
level 15, 50-1, 69, 73, 96, 110
level Linux certifications 192 liability 2
link 131, 140, 177
Linux 45, 48, 84, 159, 192-3
Linux certification 193
203
entry-level 192
Linux hacking 112, 188
Linux Operating System 45, 161
Linux system 45
Linux System 5, 45
list 94, 98, 134, 156, 191
location 12-13, 47, 154, 157, 173 lock, notebook computer 29
log-in page 19
loopholes 66
LPIC and Red Hat certifications 192

M

Mac system 55
Macintosh 55
Macintosh system 55
Macintosh System 5, 55 mail headers 43
malicious attacks 59, 144, 148, 150, 187
malicious hacker attacks 144 malicious hackers 57, 80, 163-4, 182 malwares 16, 36
Margolis, Shannon 187-90
Marketing Coordinator 188, 190 markets 102, 192
master 74-5
matter 31, 171, 182
Methods of Training for CEH Certification Exam 4, 21
Microsoft 136, 193
minds 52, 61, 63, 104, 179, 181-2, 184-5, 187, 191 mindset 178, 181, 185
mobile phone 138
modules 96, 100, 122, 156, 165, 188, 190 money 27, 29, 76, 80, 171, 173, 175 monitor 32, 109, 182, 185

Most companies 174

N

nervous system 116

networks 110, 112, 182

Network and Internet Security 69 network infrastructure 84, 86, 159, 167 network security 72
wireless 65

network security profession 161 network systems 57, 61, 72-3, 118, 167

secured 73

network traffic 30, 109 networking, wireless 65, 192 networking systems 62

204

networks 6, 13, 19, 23, 30, 32, 34, 36, 65, 104, 107, 117-18, 159, 178, 181-2, 187-8 [13]

organization's 185

neutral wireless certifications 192

non-comprehensive Certified Ethical Hacker certification 86

0

Observing systems logs 140

offline 46

offline certification 46 offline training 88-9

on-line certification 46 on-line training 70

online 5, 14-16, 27, 46, 70, 76, 89, 94, 145, 148, 175

Online CEH Certification 5, 46 online CEH certifications 46, 52 online Certification 59

online certifications 46, 60 online class 173

online games 127

online games developers 128

online schools 61

Online Schools for Certified Ethical Hackers 5, 61

online training 6, 52, 68-71, 82, 88-9, 94, 100-1, 145, 161, 165

online training courses 6, 70

Online Training Courses for Certified Ethical Hackers 70

Orchard 8, 140-1

organization network 114 organizational system 108

organizations 59, 62, 66, 71, 86, 92, 104, 107-10, 114-16, 150, 159-60, 163, 165, 179, 181, 185 [5]

organizations computer framework 185 organization's security information 163

P

pages 134-5, 149

pass 9, 17, 74, 76, 78, 80-1, 105, 120, 150, 152, 154, 159, 167, 169, 171, 173-4
passing 80, 100, 155-6, 165, 175, 188
Passive Network Recon 163 password information 34
passwords 19, 30, 38, 40-1, 45, 53, 65, 112, 129-30, 177
PDA 138-9
penetrate 12, 19, 34, 36, 45, 53, 62, 66, 73, 96, 145, 148, 150, 170, 179 penetrate computer systems 182
penetration 6, 19-20, 62, 73, 80, 82, 94, 96, 112, 166, 185 penetration test 148, 167
penetration tester 169
person 2, 16, 29, 62-3, 66, 68-70, 73, 87-8, 96, 98-9, 101, 124, 142-3, 145-7, 150, 171-4 [2]
205
personal information 16, 136
personnel security investigations (PSI) 167 phishers 177
phishing 9, 34, 129, 177
physical security 4, 12, 166, 188 platforms 50, 52, 69
multiple 52 policies 114-15
unsecured 116 popularity 192-3 presentation 156, 158
Prevent System Hacking 4, 34 preventive measures 65, 148 privacy 4, 12, 16, 27, 142
problems 49, 65, 147, 169, 173, 184
process 18-19, 30, 36, 43, 45, 53-4, 61, 92, 104, 129, 179, 185, 189 proctor 120, 152
professional certification 150, 157, 165 professional certification organization 66
Professional Security Testers Most 4
professionals 9, 76, 86, 92, 104, 110, 115, 144-5, 148, 189 proficiencies 110, 112
program 16, 48-9, 80, 129, 147, 159, 191 best Certified Ethical Hacker 80 comprehensive 122
password hacking 129
right Certified Ethical Hacker 80
Programming Certifications 110
Prometric 120, 152, 161
Prosoft Learning 191
PSI (personnel security investigations) 167 publisher 2

Q

queries 19, 25

R

range 68-9, 73, 142 reboot 23

Reference for Hacking Routers 8, 131 register 60, 62, 156
registry system 36
requirements, eligibility 120
RFID chips 28
RFID Hacking Actions 4, 28
Right Comprehensive Online Certified Ethical Hacker 90, 98 risk 8, 19, 38, 108, 127, 133, 184
Risk of VoIP Hacking 5, 38
Rootkits 36-7, 163
Router Hacking Tools 163
RSA 106

S

safeguard 61, 64, 179, 181

206

scan 14, 23, 36, 145, 159, 163, 187 scanner, web vulnerability 134-5 scanning 4, 14, 133-4, 159, 165, 188
school 13, 61, 82, 154

search 14, 142, 144

secured system 96

Securing Laptop Computers 4, 29

security 9, 12, 14-15, 20, 25, 27, 34, 39, 57, 62, 65, 68, 73-4, 144-5, 169, 192 [14]

highest level of 73

security experts 34, 38, 136

security features 38, 41

security measures 12, 25, 64, 73, 124, 131

security mechanisms 48, 55 security officers 84, 86, 159, 167 security policies 114
creating 7, 114-15

Security Professional Certifications 110

security professionals 76, 78, 82, 86, 156-7, 159, 163, 167, 189

security responses 12

security systems 107, 145, 182, 187

security systems work 150

security tester methodology, effective 96

Security Threats 6, 65, 68, 174

Security threats, potential 65

Security Training 189-90

security vulnerabilities 118, 147

fixing computer 150, 152

security walls 182, 184
self study 17, 21-2, 76, 152, 159
self-study 76, 80, 150, 154, 171, 173
server system 23
servers 25-6, 32, 64, 84
proxy 13, 127
service attacks 8, 118-19
services 2, 14, 38, 111, 118, 120, 125, 133
session hijacking 4, 15, 166
set 13, 86, 96, 100, 111, 173
Shellcoder 8, 136
shielded operating systems 45
site administrators 84, 86, 159, 167
skills 12, 31, 46, 69, 72, 76, 81-2, 84, 86, 100, 110, 112, 122, 125, 137, 144 [1]
preparatory 6, 84-5
sniffers 30, 112, 166, 188
SNMP Hacking Tools 163

207

software 14, 16, 31, 40, 52, 65, 92, 127, 131, 189 software piracy 4, 31
source 14, 43, 153, 181 spamming 17-18, 21 spoofed site 177
spot, soft 73
SQL database 19
SQL injection 19, 25, 112, 136 steal 14, 34, 138, 163
steal information 34, 36
stop 12, 15, 68, 104, 118, 124, 144-5, 177-8
stop hackers 8, 145, 148 stored information 138 strenuous work 53
students 88, 96, 152, 154-6, 161, 163, 187-90 students practice exams 165
Success Secrets 2-4
system administrators 188-9 system hackers 61
system hacking 34, 112, 166, 188
System identification/OS fingerprinting 159 system integrity verifiers 122
system manufacturers 55 system networks 165, 167-8 system security 146
organization's 150 system security analyst 34
system security measures 165 system server 25
system thief 54
systems 12-14, 19, 23-4, 36-40, 45, 52-5, 61-2, 66, 72-5, 78-81, 86-7, 107-9, 133, 159, 169-71, 187 [16]
systems administrators 22, 144 systems network 167

systems network 157
systems security 156
systems security apparatus 174
systems security practitioner 22 systems vulnerabilities 150-1

T

target computer systems 185
techniques 17-19, 25, 40, 76, 78, 80, 96, 127, 144, 154, 156, 177, 187 technologies 16-17, 29, 32-3, 38, 43, 53, 55, 102, 114, 125, 187
computing 42, 66
proxy server 4, 13 spying 32
terrorism 7, 116-17 testify 190
testing centers 62, 120, 156-7, 161
TFTP Hacking Tools 163

208

thief 30, 54, 150, 152, 167, 187, 190
threats 12, 57, 65, 68, 73, 109, 114, 116, 138, 142, 163, 169
Threats in Hacking Database Servers 8, 136
time 14-15, 27, 29, 36, 40, 72, 88, 98, 144, 147, 161, 173, 191 titles 149, 192-3
entry level 191-2
tools 12, 49, 57, 59, 64, 94, 96, 142, 152, 157, 163, 167 robust 49
Tools for Bluetooth Hacking 8, 142 track 9, 15, 28, 108-9, 148, 187, 193 trade secrets 32, 34, 168, 174
trademarks 2
train 21, 52, 86, 144, 161
trainees 74, 76, 80, 88, 94
training centers, authorized 17, 21, 144 training certification 121
training courses 7, 50-1, 70, 94, 145, 161
Trojans 36-7, 45, 112, 163, 166, 188 trust 167-8
tutorials 131-2
types 4, 12, 32, 34, 50, 74, 80, 122-3, 131, 147, 178, 184, 189

u

U3 42
Undergoing Certified Ethical Hacker 6
Undergoing Certified Ethical Hacker Training 84
Unix systems 45
USB 42, 125

USB flash drive 42

USD 157 username 129-30

users 13, 31-2, 41-2, 109, 112, 125, 177

Users of Global Positioning System 125

V

vendors 108, 192-3

victim 15, 129

Victim of Hacking Mobile Phones 8, 138 virus 14, 23, 36, 55, 188

virus scanners, free 14 viruses 14, 23, 68, 166 vision 61

Vo!P 38

Vo!P hacking 38

Vo!P Hacking 5, 38

Vo!P Hacking Tools 163

Vo!P services 38

vulnerabilities 19, 25, 28, 54, 58, 73-4, 78, 81, 86, 104, 114, 131, 134, 136-7, 142, 144 [3]

209

vulnerabilities company systems 74

Vulnerable Systems 9, 171

W

warez 4, 31

weaknesses 69, 86, 104, 131, 144, 156-7, 167, 169, 179 web 19, 40-1, 100, 152, 186, 188

web application vulnerabilities 4, 25, 112, 188

web applications 25-6, 40-1, 166 web browser 5, 53

Web Hacking Tools 163

web server administrators 64 web servers 5, 25, 64, 94

websites 13-16, 19, 34, 53, 98, 118, 120, 133-4, 169, 177

Wiley, John 8, 125

Windows Operating System 161

Wireless 163, 192 wireless networks 65

Wireless Networks Hacking 166

Wireless Networks Security 6, 65 worms 4, 23, 68

wreck havoc 5, 34, 36